Seventh International Workshop on Optimal Codes and Related Topics
September 6-12, 2013, Albena, Bulgaria *pp. 113-118*

MDS Deformations of linear codes[1]

Azniv Kasparian kasparia@fmi.uni-sofia.bg
Section of Algebra, Department of Mathematics and Informatics,
Kliment Ohridski University of Sofia
Evgeniya Velikova velikova@fmi.uni-sofia.bg
Section of Algebra, Department of Mathematics and Informatics,
Kliment Ohridski University of Sofia

Dedicated to the memory of Professor Stefan Dodunekov

Abstract. For any $\mathbb{F}_q$-linear code $C_0 \subset \mathbb{F}_q^n$ and any $[n,k,n-k+1]_q$-codes $C_1,\ldots,C_r \subset \mathbb{F}_q^n$, $r \leq q-1$, we find a family $J(f_1,\ldots,f_{n-k}) \rightarrow \mathbb{F}_q^n$ of $\mathbb{F}_q$-linear codes, depending on $f_1,\ldots,f_{n-k} \in \mathbb{F}_q[x_1,\ldots,x_n]$ and containing $C_0,C_1,\ldots,C_r$ as some of its fibers. For any family $J(f_1,\ldots,f_{n-k}) \rightarrow \mathbb{F}_q^n$ with k-dimensional fibers is shown the existence of an affine variety $X \subset \overline{\mathbb{F}_q}^n$, defined over $\mathbb{F}_q$, whose $\mathbb{F}_q$-Zariski tangent bundle $T^{\mathbb{F}_q}X|_{X^{\mathrm{smooth}}(\mathbb{F}_q)}$ coincides with $J(f_1,\ldots f_{n-k})|_{X^{\mathrm{smooth}}(\mathbb{F}_q)}$ over the smooth $\mathbb{F}_q$-rational locus $X^{\mathrm{smooth}}(\mathbb{F}_q)$ of X. The variety X can be chosen in such a way that to require $T^{\mathbb{F}_q}X|_{X^{\mathrm{smooth}}(\mathbb{F}_q)}$ to pass through $r \leq q$ MDS-fibers of $J(f_1,\ldots,f_{n-k})$. If $T^{\mathbb{F}_q}X|_{X^{\mathrm{smooth}}(\mathbb{F}_q)}$ has an MDS-member $T_a^{\mathbb{F}_q}X \simeq \mathbb{F}_q^k$ then all the projections of $X \subset \overline{\mathbb{F}_q}^n$ in the k-dimensional coordinate subspaces of $\overline{\mathbb{F}_q}^n$ have to be dominant. This global geometric property of X is proved to be sufficient for the presence of an MDS-fiber $T_a^{\mathbb{F}_{q^m}}X$ over a sufficiently large extension $\mathbb{F}_{q^m} \supseteq \mathbb{F}_q$.

All codes, considered in the present note are linear. We say that C is an $[n,k,d]_q$-code if $C \subset \mathbb{F}_q^n$ is of length n, dimension k and minimum distance d. Singleton bound asserts that $d \leq n+1-k$. A code C is referred to as an MDS-one (Maximum Distance Separable) if $d = n+1-k$.

For $\forall f_1,\ldots,f_{n-k} \in \mathbb{F}_q[x_1,\ldots,x_n]$, $\forall a \in \mathbb{F}_q^n$ consider the Jacobian matrix

$$\frac{\partial(f_1,\ldots,f_{n-k})}{\partial(x_1,\ldots,x_n)} = \begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \ldots & \frac{\partial f_1}{\partial x_n} \\ \ldots & \ldots & \ldots \\ \frac{\partial f_{n-k}}{\partial x_1} & \ldots & \frac{\partial f_{n-k}}{\partial x_n} \end{pmatrix}$$

and the solution space $J(f_1,\ldots,f_{n-k})_a \subset \mathbb{F}_q^n$ of the homogeneous linear system with matrix $\frac{\partial(f_1,\ldots,f_{n-k})}{\partial(x_1,\ldots,x_n)}(a)$. The Jacobian family $J(f_1,\ldots,f_{n-k}) \rightarrow \mathbb{F}_q^n$ is the union $J(f_1,\ldots,f_{n-k}) := \cup_{a\in\mathbb{F}_q^n} J(f_1,\ldots,f_{n-k})_a$.

If $\overline{\mathbb{F}_q} = \cup_{m=1}^{\infty}\mathbb{F}_{q^m}$ is the algebraic closure of $\mathbb{F}_q$ and $g_1,\ldots,g_m \in \mathbb{F}_q[x_1,\ldots,x_n]$, then $X = V(g_1,\ldots,g_m) := \{a \in \overline{\mathbb{F}_q}^n \,|\, g_i(a_1,\ldots,a_n) = 0, \forall 1 \leq i \leq m\}$ is

[1]This research is partially supported by Contract 101/19.04.2013.

called an affine variety, defined over $\mathbb{F}_q$ and $X(\mathbb{F}_q) := X \cap \mathbb{F}_q^n$ is the set of the $\mathbb{F}_q$-rational points of X. One defines the $\mathbb{F}_q$-Zariski tangent space to X at $a \in X(\mathbb{F}_q)$ as $T_a^{\mathbb{F}_q} X = J(h_1, \dots, h_s)_a$ for any generating set $h_1, \dots, h_s$ of $I(X) := \{h \in \mathbb{F}_q[x_1, \dots, x_n] \mid h(a) = 0 \text{ for } \forall a \in X\} \supseteq \langle g_1, \dots, g_m \rangle_{\mathbb{F}_q}$.

1 Existence of MDS-deformations

Proposition 1. *Let $\mathbb{F}_q = \{t_0 = 0, t_1, \dots, t_{q-1}\}$, $A^{(0)} \in Mat_{(n-k)\times n}(\mathbb{F}_q)$ be a check matrix of a code $C_0 \subset \mathbb{F}_q^n$ and $A^{(1)}, \dots, A^{(r)} \in Mat_{(n-k)\times n}(\mathbb{F}_q)$ be check matrices of $[n, k, n-k+1]_q$-codes $C_1, \dots, C_r$ for some $r \leq q-1$. If $L_i(x) = \frac{(x-t_0)\dots(x-t_{i-1})(x-t_{i+1})\dots(x-t_r)}{(t_i-t_0)\dots(t_i-t_{i-1})(t_i-t_{i+1})\dots(t_i-t_r)}$, $0 \leq i \leq r$ are the Lagrange basis polynomials and $\Phi_p : \mathbb{F}_q \to \mathbb{F}_q$, $\Phi_p(t) = t^p$ is the Frobenius automorphism then the Jacobian family $J(f_1, \dots, f_{n-k}) \to \mathbb{F}_q^n$ of $f_s(x_1, \dots, x_n) = \sum_{j=1}^{n} \sum_{i=0}^{r} A_{sj}^{(i)} x_j L_j(x_j^p)$, $1 \leq s \leq n-k$ is a deformation of $J(f_1, \dots, f_{n-k})_{(0,\dots,0)} = C_0$ with $[n, k, n-k+1]_q$-fibers $J(f_1, \dots, f_{n-k})_{(\Phi_p^{-1}(t_i),\dots,\Phi_p^{-1}(t_i))} = C_i$ for $\forall 1 \leq i \leq r$.*

In the case of $r = q-1$, $f_s(x_1, \dots, x_n) = \sum_{j=1}^{n} \sum_{i=0}^{q-1} A_{sj}^{(i)} x_j \left[\sum_{m=0}^{q-1} t_i^{q-1-m} x_j^{pm} - 1\right]$.

Proof. If $A^{(i)} = (A_1^{(i)} \dots A_n^{(i)})$ with $A_j^{(i)} \in Mat_{(n-k)\times 1}(\mathbb{F}_q)$ then the polynomial family of points $H_j(x_j) = \sum_{i=0}^{r} A_j^{(i)} L_i(x_j^p) \in Mat_{(n-k)\times 1}(\mathbb{F}_q[x_j])$ passes through $H_j(\Phi_p^{-1}(t_i)) = A_j^{(i)}$ for $\forall 0 \leq i \leq r$. According to $\frac{\partial(x_j L_i(x_j^p))}{\partial x_j} = L_i(x_j^p)$, the Jacobian matrix $\frac{\partial(f_1,\dots,f_{n-k})}{\partial(x_1,\dots,x_n)} = (H_1(x_1) \dots H_n(x_n))$ and the fibers $J(f_1, \dots, f_{n-k})_{(\Phi_p^{-1}(t_i),\dots,\Phi_p^{-1}(t_i))} = C_i$ for $\forall 0 \leq i \leq r$.

In the case of $r = q-1$, the elementary symmetric polynomials $\sigma_s = \sum_{0 \leq i_1 < \dots < i_s \leq q-1} t_{i_1} \dots t_{i_s}$, $1 \leq s \leq q$ of $t_0, t_1, \dots, t_{q-1}$ and the elementary symmetric polynomials $\tau_s = \sum_{i_1 < \dots < i_s, i \notin \{i_1,\dots,i_s\}} t_{i_1} \dots t_{i_s}$, $1 \leq s \leq q-1$ of $t_0, \dots, t_{i-1}, t_{i+1}, \dots, t_{q-1}$ satisfy the equalities $\sigma_1 = \tau_1 + t_1$ and $\sigma_s = \tau_s + t_i \tau_{s-1}$ for $2 \leq s \leq q-1$. Then $x^q - x = \prod_{\nu=0}^{q-1}(x - t_\nu) = x^q + \sum_{m=0}^{q-1}(-1)^{q-m}\sigma_{q-m}x^m$ specifies that $\sigma_1 = \dots = \sigma_{q-2} = 0$, $\sigma_{q-1} = (-1)^q$, $\sigma_q = 0$. By an induction on $1 \leq s \leq q-2$, there holds $\tau_s = (-t_i)^s$ for $\forall 1 \leq s \leq q-2$. Combining with $\tau_{q-1} = (-1)^{q-1}(t_i^{q-1} - 1)$, one gets $\Lambda_i(x) = \prod_{j \neq i}(x - t_j) = x^{q-1} + \sum_{m=0}^{q-2}(-1)^{q-1-m}\tau_{q-1-m}x^m = \sum_{m=0}^{q-1} t_i^{q-1-m} x^m - 1$. Thus, $\Lambda_i(t_i) = -1$ and

$-L_i(x) = -\frac{\Lambda_i(x)}{\Lambda_i(t_i)} = \Lambda_i(x) = \sum\limits_{m=0}^{q-1} t_i^{q-1-m} x^m - 1$. One can replace f_s by $-f_s$.

$\square$

The columns of the check matrices of $[n,k,n-k+1]_q$-codes consist of homogeneous coordinates of n-arcs in $\mathbb{P}^{n-k}(\mathbb{F}_q)$. In order to formulate the counterpart of Proposition 1 for arcs, let us consider the $\mathbb{F}_q^*$-action on $\mathbb{F}_q[x_1,\dots,x_n]^{n-k}$ by $(\lambda,(f_1,\dots,f_{n-k})) \mapsto (\lambda f_1,\dots,\lambda f_{n-k})$ for $\lambda \in \mathbb{F}_q^*$, $f_1,\dots,f_{n-k} \in \mathbb{F}_q[x_1,\dots,x_n]$ and the orbit space $\mathbb{F}_q[x_1,\dots,x_n]^{n-k}/\mathbb{F}_q^* \ni [f_1 : \dots : f_{n-k}]$. If $p = \mathrm{char}(\mathbb{F}_q)$ then the derivations

$$\frac{\partial}{\partial x_j}\left(\sum_\alpha c_\alpha x_1^{\alpha_1}\dots x_j^{\alpha_j}\dots x_n^{\alpha_n}\right) = \sum_\alpha c_\alpha x_1^{\alpha_1}\dots[\alpha_j (\mathrm{mod}\, p)] x_j^{\alpha_j-1}\dots x_n^{\alpha_n},$$

$1 \le j \le n$ commute with the $\mathbb{F}_q^*$-action and descend to maps

$$\frac{\partial}{\partial x_j} : \mathbb{F}_q[x_1,\dots,x_n]^{n-k}/\mathbb{F}_q^* \longrightarrow \mathbb{F}_q[x_1,\dots,x_n]^{n-k}/\mathbb{F}_q^*.$$

For any $a \in \mathbb{F}_q^n$ let

$$\mathcal{E}_a : \mathbb{F}_q[x_1,\dots,x_n]^{n-k}/\mathbb{F}_q^* \longrightarrow \mathbb{F}_q^{n-k}/\mathbb{F}_q^* = \mathbb{P}^{n-k}(\mathbb{F}_q) \cup \{[0:\dots:0]\},$$

$\mathcal{E}_a([f_1:\dots:f_{n-k}]) = [f_1(a):\dots:f_{n-k}(a)]$ be the evaluation map at a

Corollary 1. *Any n-arcs $\mathcal{A}_i = \{P_1^{(i)},\dots,P_n^{(i)}\} \subset \mathbb{P}^{n-k}(\mathbb{F}_q)$, $1 \le i \le r \le q$ admit an integrable polynomial interpolation. Namely, there exists some $f = [f_1:\dots:f_{n-k}] \in \mathbb{F}_q[x_1,\dots,x_n]^{n-k}/\mathbb{F}_q^*$ with $(\mathcal{E}_{(\Phi_p^{-1}(t_i),\dots,\Phi_p^{-1}(t_i))} \circ \frac{\partial}{\partial x_j})(f) = P_j^{(i)}$ for $\forall 1 \le j \le n$, $\forall \le i \le r$, $\mathbb{F}_q = \{t_1,\dots,t_q\}$ and $\Phi_p : \mathbb{F}_q \to \mathbb{F}_q$, $\Phi_p(t) = t^p$.*

Example 1. *Let $S_d = S_d(x_1,\dots,x_{n-1}) = \sum\limits_{\nu=1}^{n-1} x_\nu^d$. Consider $\Sigma_i = S_{(i-1)p+1}$ for $1 \le i \le n-k-1$, $\Sigma_{n-k} = S_{(n-k-1)p+1} + x_n$ and $J(\Sigma_1,\dots,\Sigma_{n-k}) \to \mathbb{F}_q^n$ for some $1 \le n \le q+1$. The fibers $J(\Sigma_1,\dots,\Sigma_{n-k})_a$ with $a_i \ne a_j$ for all $1 \le i < j \le n-1$ are $[n,k,n-k+1]_q$-codes. If $a' = (a_1,\dots,a_{n-1}) \in \mathbb{F}_q^{n-1}$ has $n-k \le t \le n-2$ different components then $J(\Sigma_1,\dots,\Sigma_{n-k})_{(a',a_n)}$ is an $[n,k,2]_q$-code for $\forall a_n \in \mathbb{F}_q$. When $a' \in \mathbb{F}_q^{n-1}$ has $1 \le t < n-k$ different components, the fiber $J(\Sigma_1,\dots,\Sigma_{n-k})_{(a',a_n)}$ is an $[n,n-t,2]_q$-code with $n-t > k$.*

Towards an explanation of Example 1, let us note that the Jacobian matrix

$$\frac{\partial(\Sigma_1,\dots,\Sigma_{n-k})}{\partial(x_1,\dots,x_n)} = \begin{pmatrix} 1 & \dots & 1 & 0 \\ x_1^p & \dots & x_{n-1}^p & 0 \\ \dots & \dots & \dots & \dots \\ x_1^{(n-k-2)p} & \dots & x_{n-1}^{(n-k-2)p} & 0 \\ x_1^{(n-k-1)p} & \dots & x_{n-1}^{(n-k-1)p} & 1 \end{pmatrix}.$$

The projectivizations of the columns of the above matrix belong to a rational normal curve in $\mathbb{P}^{n-k}(\mathbb{F}_q)$ and form an arc for different $x_1, \ldots, x_{n-1} \in \mathbb{F}_q$.

2 The MDS-families as Zariski tangent bundles

If $X = V(f_1, \ldots, f_{n-k}) \subset \overline{\mathbb{F}_q}^n$ is of $\dim X = k$ and $J(f_1, \ldots, f_{n-k})$ if of constant rank k, then $J(f_1, \ldots, f_{n-k})_a = T_a^{\mathbb{F}_q} X$ for $\forall a \in X^{\mathrm{smooth}}(\mathbb{F}_q)$ with an eventually strict inclusion $\langle f_1, \ldots, f_{n-k} \rangle \subseteq I(X)$. The next proposition realizes $J(f_1, \ldots, f_{n-k}) \to \mathbb{F}_q^n$ as an $\mathbb{F}_q$-Zariski tangent bundle for arbitrary $\dim V(f_1, \ldots, f_{n-k}) \geq k$.

Proposition 2. *Suppose that $J(f_1, \ldots, f_{n-k}) \to \mathbb{F}_q^n$ has $\dim_{\mathbb{F}_q} J(f_1, \ldots, f_{n-k}) = k$ for $\forall a \in S_o \subseteq \mathbb{F}_q^n$, $D = \max(\deg(f_1), \ldots, \deg(f_{n-k}))$, $p = \mathrm{char}(\mathbb{F}_q)$ and $g_s = f_s + x_s^{pD}$ for $1 \leq s \leq n-k$. Then $X = V(g_1, \ldots, g_{n-k})$ is an affine variety of $\dim X = k$, $S_o \cap X = S_o \cap X(\mathbb{F}_q)$ is contained in $X^{\mathrm{smooth}}(\mathbb{F}_q)$ and $J(f_1, \ldots, f_{n-k})_a = J(g_1, \ldots, g_{n-k})_a = T_a^{\mathbb{F}_q} X$ for $\forall a \in S_o \cap X$.*

Proof. Note that $J(f_1 + x_1^{pD}, \ldots, f_{n-k} + x_{n-k}^{pD})_a = J(f_1, \ldots, f_{n-k})_a$ for $\forall a \in \mathbb{F}_q^n$ by $\frac{\partial(f_1 + x_1^{pD}, \ldots, f_{n-k} + x_{n-k}^{pD})}{\partial(x_1, \ldots, x_n)} \equiv \frac{\partial(f_1, \ldots, f_{n-k})}{\partial(x_1, \ldots, x_n)}$. Let $I := \langle g_1, \ldots, g_s \rangle_{\mathbb{F}_q}$, $X = V(I)$, $I(X) = \langle h_1, \ldots, h_m \rangle_{\mathbb{F}_q}$. Then $T^{\mathbb{F}_q} X := \cup_{a \in X(\mathbb{F}_q)} T_a^{\mathbb{F}_q} X = J(h_1, \ldots, h_m)|_{X(\mathbb{F}_q)}$ and $I \subseteq I(X)$ implies the fiberwise inclusion $T^{\mathbb{F}_q} X \subseteq J(f_1, \ldots, f_{n-k})|_{X(\mathbb{F}_q)}$. It suffices to show that $\dim X = k$ towards $T_a^{\mathbb{F}_q} X = J(f_1, \ldots, f_{n-k})_a$ for all $a \in S_o \cap X = S_o \cap X(\mathbb{F}_q)$ and $S_o \cap X \subseteq X^{\mathrm{smooth}}(\mathbb{F}_q)$.

For any $\Sigma \subseteq \mathbb{F}_q[x_1, \ldots, x_n]$ let $\Sigma^{(s)} := \{f \in \Sigma | \deg f \leq s\}$. By Prop.3, p.428 [1] and Prop.4, p.428 [1], for sufficiently large s the function $HP_{I(X)}(s) := \dim_{\mathbb{F}_q} \mathbb{F}_q[x_1, \ldots, x_n]^{(s)} - \dim_{\mathbb{F}_q} I(X)^{(s)}$ is a polynomial of s, called the Hilbert polynomial of X. Thm.6, p.451 [1] and Def.7, p.430 [1] imply that $\dim X = \deg HP_{I(X)}$. Prop.6, p.430. [1] provides $HP_{I(X)}(s) = HP_I(s)$, whereas $\dim X = \deg HP_I(s)$. Let $\succ$ be the graded monomial order with respect to which $x^\alpha \succ x^\beta$ if and only if $\sum_{i=1}^n \alpha_i > \sum_{i=1}^n \beta_i$ or $\sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i$, $\alpha_1 = \beta_1, \ldots, \alpha_{j-1} = \beta_{j-1}, \alpha_j > \beta_j$ for some $1 \leq j \leq n$. The ideal $LT(I) := \langle LT(f) | f \in I \rangle_{\mathbb{F}_q}$ of the leading terms of I has Hilbert polynomial $HP_{LT(I)}(s) = HP_I(s)$ by Prop.4, p.421 [1]. According to Prop.6, p.430 and Def.7, p.430, $\dim X = \deg HP_{LT(I)} = \deg HP_{I(V(LT(I)))} = \dim V(LT(I))$. However, $LT(g_s) = x_s^{pD} \in LT(I)$, $\forall 1 \leq s \leq n-k$ implies $V(LT(I)) \subseteq V(x_1^{pD}, \ldots, x_{n-k}^{pD}) \simeq \mathbb{F}_q^k$, so that $\dim X = \dim V(LT(I)) \leq k$ and $\dim X = k$.

$\square$

Corollary 2. *Suppose that* $J(f_1,\dots,f_{n-k}) \to \mathbb{F}_q^n$ *has* $\dim_{\mathbb{F}_q} J(f_1,\dots,f_{n-k})_a = k$ *for* $\forall a \in S_o \subseteq \mathbb{F}_q^n$ *and* $[n,k,n-k+1]_q$*-fibers* $J(f_1,\dots,f_{n-k})_{a^{(\lambda)}}$, $1 \leq \lambda \leq r \leq q$. *If* $a_{j_s}^{(1)},\dots,a_{j_s}^{(r)} \in \mathbb{F}_q^*$ *are different for* $\forall j_s \in \{j_1,\dots,j_{n-k}\}$, $j_1 < \dots < j_{n-k}$ *and* $\{a^{(1)},\dots a^{(r)}\} \not\subseteq V(f_\nu)$, $\forall 1 \leq \nu \leq n-k$, *then one can find polynomials* $g_s = f_s + \sum_{\delta=D}^{D+r-1} c_{s,\delta} x_{j_s}^{p\delta} \in \mathbb{F}_q[x_1,\dots,x_n]$, $1 \leq s \leq n-k$, *cutting a* k*-dimensional affine variety* $X = V(g_1,\dots,g_{n-k}) \subset \overline{\mathbb{F}_q}^n$, *defined over* $\mathbb{F}_q$, *with* $a^{(1)},\dots,a^{(r)} \in S_o \cap X$ *and* $J(f_1,\dots,f_{n-k})_a = J(g_1,\dots,g_{n-k})_a = T_a^{\mathbb{F}_q} X$ *for all* $a \in S_o \cap X$.

Proof. By the proof of Proposition 2, $\dim X = k$ under the presence of at least one $c_{s,\delta} \neq 0$ for any $1 \leq s \leq n-k$. Towards $a^{(\lambda)} \in S_o \cap X$ for $\forall 1 \leq \lambda \leq r$, the undetermined coefficients $c_{s,\delta} \in \mathbb{F}_q$ have to satisfy $\sum_{\delta=D}^{D+r-1} c_{s,\delta}(a_{j_s}^{(\lambda)})^{p\delta} = -f_s(a^{(\lambda)})$, $1 \leq \lambda \leq r$. The coefficient matrix of that linear system has determinant $(a_{j_s}^{(1)} \dots a_{j_s}^{(r)})^{pD} \prod_{r \geq \lambda > \mu \geq 1} \left[\left(a_{j_s}^{(\lambda)}\right)^p - \left(a_{j_s}^{(\mu)}\right)^p \right] \neq 0$, as far as $\Phi_p(a_{j_s}^{(\lambda)}) \neq \Phi_p(a_{j_s}^{(\mu)})$ for $a_{j_s}^{(\lambda)} \neq a_{j_s}^{(\mu)}$ and $\Phi_p(t) = t^p$, $t \in \mathbb{F}_q$.

$\square$

Assume that C_0 from Proposition 1 is an $[n,k,n-k+1]_q$-code. Then Corollary 2 applies to $J(f_1,\dots,f_{n-k}) \to \mathbb{F}_q^n$ and provides an affine variety X, defined over $\mathbb{F}_q$ with at least $r \leq q$ $\mathbb{F}_q$-Zariski tangent spaces, which are MDS-codes.

Let $\mathbb{F}_q = \{t_0 = 0, t_1,\dots,t_{q-1}\}$, $\zeta = (0,1,\dots,q-1) \in \mathrm{Sym}(q)$ and $b_i = (t_{\zeta^i(0)},\dots,t_{\zeta^i(n-2)},\theta_i)$, $1 \leq i \leq q$ for some $\theta_i \in \mathbb{F}_q$. The application of Corollary 2 to $J(\Sigma_1,\dots,\Sigma_{n-k})$ from Example 1 and its fibers over $b_1,\dots,b_q$ implies the existence of an affine variety X, defined over $\mathbb{F}_q$ with at least q $\mathbb{F}_q$-Zariski tangent spaces, which are MDS-codes.

Proposition 3. *Let* $X = V(I) \subset \overline{\mathbb{F}_q}^n$, $I \triangleleft \mathbb{F}_q[x_1,\dots,x_n]$ *be an irreducible affine variety of* $\dim X = k$, *defined over* $\mathbb{F}_q$. *For any* $i = (i_1,\dots,i_k)$ *with* $1 \leq i_1 < \dots < i_k \leq n$, $\{j_1,\dots,j_{n-k}\} = \{1,\dots,n\} \setminus \{i_1,\dots,i_k\}$, $1 \leq j_1 < \dots < j_{n-k} \leq n$ *consider the projection* $\Pi_i : X \to \overline{\mathbb{F}_q}^k$, $\Pi_i(x_1,\dots,x_n) = (x_{i_1},\dots,x_{i_k})$ *and a Groebner basis* G_i *of* $I \triangleleft \mathbb{F}_q[x_1,\dots,x_n]$ *with respect to the lexicographic order* $\succ$ *of* $\mathbb{F}_q[x_1,\dots,x_n]$ *with* $x_{j_1} \succ \dots \succ x_{j_{n-k}} \succ x_{i_1} \succ \dots \succ x_{i_k}$.

(i) If $a \in X^{\mathrm{smooth}}(\mathbb{F}_q)$ *has smooth images* $\Pi_i(a) \in \Pi_i(X)$ *for* $\forall i$ *and* $T_a^{\mathbb{F}_q} X$ *is an* $[n,k,n-k+1]_q$*-code, then* $G_i \cap \mathbb{F}_q[x_{i_1},\dots,x_{i_k}] = \emptyset$ *for* $\forall i = (i_1,\dots,i_k)$.

(ii) If $G_i \cap \mathbb{F}_q[x_{i_1},\dots,x_{i_k}] = \emptyset$ *for* $\forall i$ *then there is* $N \in \mathbb{N}$, *depending on the embedding of* X *in* $\overline{\mathbb{F}_q}^n$, *such that for* $\forall m \in \mathbb{N}$ *with* $q^m > N$ *at least one* $\mathbb{F}_{q^m}$*-Zariski tangent space* $T_a^{\mathbb{F}_{q^m}} X$, $a \in X^{\mathrm{smooth}}(\mathbb{F}_{q^m})$ *is an* $[n,k,n-k+1]_q$*-code.*

Proof. A morphism $\varphi : Y \to Z$ is dominant when $\varphi(Y)$ is not contained in a proper affine subvariety of Z. We claim that $\Pi_i : X \to \overline{\mathbb{F}_q}^k$, $\Pi_i(x_1, \ldots, x_n) = (x_{i_1}, \ldots, x_{i_k})$ is dominant if and only if $G_i \cap \mathbb{F}_q[x_{i_1}, \ldots, x_{i_k}] = \emptyset$. To this end, let $I_j := I \cap \mathbb{F}_q[x_{i_1}, \ldots, x_{i_k}]$ and note that $V(I_j)$ is the Zariski closure of $\Pi_i(X)$ by the proof of Thm.3, p.123 [1]. The Elimination Thm.2, p.114 [1] asserts that $G_i \cap \mathbb{F}_q[x_{i_1}, \ldots, x_{i_k}]$ is a Groebner basis of I_j. Thus, $G_i \cap \mathbb{F}_q[x_{i_1}, \ldots, x_{i_k}] = \emptyset$ is equivalent to $I_j = \{0\}$ which, in turn, holds exactly when $V(I_j) = \overline{\mathbb{F}_q}^k$.

A morphism $\varphi : Y \to \varphi(Y)$ is etale at $a \in Y$ if $d\varphi_p : T_p^{\mathbb{F}_q} Y \to T_{\varphi(p)}^{\mathbb{F}_q} \varphi(Y)$ is an $\mathbb{F}_q$-linear isomorphism. Thus, $T_a^{\mathbb{F}_q} X$, $a \in X^{\text{smooth}}(\mathbb{F}_q)$ is an $[n, k, n-k+1]_q$-code exactly when Π_i are etale at a for $\forall i$. More precisely, $T_a^{\mathbb{F}_q} X$ is an MDS-code if an only if for any i there exist homogeneous linear functions $v_{j_r}(v_{i_1}, \ldots, v_{i_k})$, $1 \leq r \leq n-k$ with $T_a^{\mathbb{F}_q} X = \{v = (v_1, \ldots, v_n) \,|\, \forall (v_{i_1}, \ldots, v_{i_k}) \in \mathbb{F}_q^k\}$. The last condition is equivalent to the invertibility of $d_a \Pi_i : T_a^{\mathbb{F}_q} X \to \mathbb{F}_q^k$ for $\forall i$.

(i) If Π_i is etale at $a \in X^{\text{smooth}}(\mathbb{F}_q)$ then $\mathbb{F}_q^k = d_a \Pi_i (T_a^{\mathbb{F}_q} X) \subseteq T_{\Pi_i(a)}^{\mathbb{F}_q} \Pi_i(X)$ requires $T_{\Pi_i(a)}^{\mathbb{F}_q} \Pi_i(X) = \mathbb{F}_q^k$. For a smooth point $\Pi_i(a) \in \Pi_i(X)^{\text{smooth}}$ that suffices for $\dim \Pi_i(X) = k$ and holds exactly when Π_i is dominant.

(ii) The dominant morphism $\Pi_i : X \to \overline{\mathbb{F}_q}^k$ of an irreducible X induces an embedding $\overline{\mathbb{F}_q}(x_{i_1}, \ldots, x_{i_k}) \hookrightarrow \overline{\mathbb{F}_q}(X)$ of the function fields. Due to $\dim X = k$, $[\overline{\mathbb{F}_q}(X) : \overline{\mathbb{F}_q}(x_{i_1}, \ldots, x_{i_k})] < \infty$ and Π_i has finite fibers. If $R_i \subset \overline{\mathbb{F}_q}^k$ is the branch locus of Π_i, then $\Pi_i : \Pi_i^{-1}(\overline{\mathbb{F}_q}^k \setminus R_i) \longrightarrow \overline{\mathbb{F}_q}^k \setminus R_i$ is an etale covering. Let $I^{\overline{\mathbb{F}_q}}(X)$ be the ideal of X over $\overline{\mathbb{F}_q}$. If $\Pi_{j_s,i} : X \to \overline{\mathbb{F}_q}^{k+1}$, $\Pi_{j_s,i}(x_1, \ldots, x_n) = (x_{j_s}, x_{i_1}, \ldots, x_{i_k})$, $\pi_{j_s} : \Pi_{j_s,i}(X) \to \Pi_i(X)$, $\pi_{j_s}(x_{j_s}, x_{i_1}, \ldots, x_{i_k}) = (x_{i_1}, \ldots, x_{i_k})$ and R_{j_s} is the branch locus of π_{j_s} then $R_i = \cup_{s=1}^{n-k} R_{j_s}$. For $\forall j_s \in \{1, \ldots, n\} \setminus \{i_1, \ldots, i_k\}$ there is $\varphi_{j_s} \in \{\overline{\mathbb{F}_q}[x_{i_1}, \ldots, x_{i_k}][x_{j_s}] \cap I^{\overline{\mathbb{F}_q}}(X)\} \setminus \{0\}$ with $\Pi_{j_s,i}(X) = \{(x_{j_s}, x_{i_1}, \ldots, x_{i_k}) \in \overline{\mathbb{F}_q}^{k+1} \,|\, \varphi_{j_s}(x_{j_s}) = 0\}$. If $d_{j_s} \in \mathbb{N}$ is the total degree of the discriminant $D(\varphi_{j_s}) \in \overline{\mathbb{F}_q}[x_{i_1}, \ldots, x_{i_k}]$ then $R_{j_s} = \{(x_{i_1}, \ldots, x_{i_k}) \in \overline{\mathbb{F}_q}^k \,|\, D(\varphi_{j_s})(x_{i_1}, \ldots, x_{i_k}) = 0\}$ has $|R_{j_s}(\mathbb{F}_{q^m})| \leq d_{j_s} q^{m(k-1)}$. Thus, $|R_i(\mathbb{F}_{q^m}| \leq \left(\sum_{s=1}^{n-k} d_{j_s} \right) q^{m(k-1)} < q^{mk} = |\mathbb{F}_{q^m}^k|$ for $q^m > N := \sum_{s=1}^{n-k} d_{j_s}$ and $R_i(\mathbb{F}_{q^m}) \subsetneq \mathbb{F}_{q^m}^k$. $\square$

References

[1] D. Cox, J. Little and D. O'Shea, *Ideals, varieties, and Algorithms - An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Springer, 1992.