Intersections between the norm-trace curve and some low degree curves

Matteo Bonini, Massimiliano Sala

Abstract

In this paper we analyze the intersection between the norm-trace curve over $\mathbb{F}_{q^3}$ and the curves of the form $y = ax^3 + bx^2 + cx + d$, giving a complete characterization of the intersection between the curve and the parabolas (a=0), as well as sharp bounds for the other cases. This information is used for the determination of the weight distribution of some one-point AG codes arising from the curve.

Keywords: Norm-trace curve - AG Code - Weight distribution
MSC Codes: 14G50 - 11T71 - 94B27

1 Introduction

Algebraic Geometry (AG codes for short) codes form an important class of error correcting codes; see [11, 12, 27].

Let $\mathcal{X}$ be an algebraic curve defined over the finite field $\mathbb{F}_q$ of order q. The parameters of the AG codes associated with $\mathcal{X}$ strictly depend on some properties of the underlying curve $\mathcal{X}$. In general, curves with many $\mathbb{F}_q$-rational places with respect to their genus give rise to AG codes with good parameters. For this reason, maximal curves, that is, curves attaining the Hasse-Weil upper bound, have been widely investigated in the literature; see for instance [3, 4, 22, 26, 28–30].

The determination of the intersection of a given curve $\mathcal{X}$ and low degree curves is often useful for the determination of the weight distribution of the AG code arising from $\mathcal{X}$; see [1, 2, 8, 19, 20].

The norm-trace curve is a natural generalization of the Hermitian curve to any extension field $\mathbb{F}_{q^r}$. It has been widely studied for coding theoretical purposes; see [1, 10, 15, 21, 23, 24].

In this paper, we focus on the intersection between the norm-trace curves and curves of the form $y = ax^3 + bx^2 + cx + d$ over $\mathbb{F}_{q^3}$. We characterize the intersection between the norm-trace curve and parabolas and we provide tools to get sharp bounds in the other cases. To do so we

investigate specific irreducible surfaces over finite fields. In addition, we partially deduce the weight distribution of the corresponding one-point codes.

2 Preliminary Results

Throughout the paper, let p be a prime and $q = p^m$, where m is a positive integer. Let $\mathbb{F}_q$ be the finite field with q elements. An $[n, k, d]$ linear code $\mathcal{C}$ over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$ with minimum Hamming distance d. Let A_i be the number of codewords with Hamming weight i in $\mathcal{C}$.

2.1 The norm-trace curve

The *norm-trace curve* $\mathcal{X}$ is the plane curve defined over $\mathbb{F}_{q^r}$ by the affine equation

$$x^{\frac{q^r-1}{q-1}} = y^{q^{r-1}} + y^{q^{r-2}} + \cdots + y^q + y. \tag{1}$$

The *norm* $\mathrm{N}_{\mathbb{F}_q}^{\mathbb{F}_{q^r}}$ and the *trace* $\mathrm{T}_{\mathbb{F}_q}^{\mathbb{F}_{q^r}}$ are two well-known functions from $\mathbb{F}_{q^r}$ to $\mathbb{F}_q$ such that

$$\mathrm{N}_{\mathbb{F}_q}^{\mathbb{F}_{q^r}}(x) = x^{\frac{q^r-1}{q-1}} = x^{q^{r-1}+q^{r-2}+\cdots+q+1}$$

and

$$\mathrm{T}_{\mathbb{F}_q}^{\mathbb{F}_{q^r}}(x) = x^{q^{r-1}} + x^{q^{r-2}} + \cdots + x^q + x.$$

When q and r are understood, we will write $\mathrm{N} = \mathrm{N}_{\mathbb{F}_q}^{\mathbb{F}_{q^r}}$ and $\mathrm{T} = \mathrm{T}_{\mathbb{F}_q}^{\mathbb{F}_{q^r}}$.

The equation $x^{\frac{q^r-1}{q-1}} = y^{q^{r-1}} + y^{q^{r-2}} + \cdots + y^q + y$ has precisely q^{2r-1} solutions in $\mathbb{A}^2(\mathbb{F}_{q^r})$, so the curve $\mathcal{X}$ has $q^{2r-1}+1$ rational points: q^{2r-1} of them correspond to affine places, plus a single place at the infinity P_∞.

If $r = 2$, $\mathcal{X}$ coincides with the Hermitian curve and if $r \geq 3$ $\mathcal{X}$ is singular in P_∞.

Moreover it is known that its Weierstrass semigroup in P_∞ is generated by $\left\langle q^{r-1}, \frac{q^r-1}{q-1} \right\rangle$, see [10].

Our main aim is the study of the intersection between $\mathcal{X}$ and cubics of the form $y = ax^3 + bx^2 + cx + d$, where $a, b, c, d \in \mathbb{F}_{q^r}$. In particular, we focus on the intersections between $\mathcal{X}$ and parabolas. The case $r = 2$ and $a = 0$ is completely investigated in [9, 19], so we deal with the more difficult case $r \geq 3$. We set the problem for the general case in Section 3, while in the rest of the paper we concentrate on the solution to the case $r = 3$ and $a = 0$, obtaining partial results for the case $a \neq 0$ in Section 6.

2.2 Algebraic Geometry Codes

We introduce here some basic notions on AG codes; for a detailed introduction to this topic, we refer to [27, Chapter 2].

Let $\mathbb{F}_q$ be the finite field with q elements and $\mathcal{X}$ be a projective, absolutely irreducible, algebraic curve of genus g defined over $\mathbb{F}_q$. Let $\mathbb{F}_q(\mathcal{X})$ be the field of rational functions on $\mathcal{X}$ and $\mathcal{X}(\mathbb{F}_q)$ be the set of rational places of $\mathcal{X}$. For any divisor $D = \sum_{P \in \mathcal{X}(\overline{\mathbb{F}}_q)} m_P P$ on $\mathcal{X}$, we denote by $v_P(D)$ the valuation $m_P \in \mathbb{Z}$ of D at P, and by $\mathrm{supp}(D)$ the support of D; the degree of D is $\deg(D) = \sum_{P \in \mathrm{supp}(D)} n_P$. The Riemann-Roch space $\mathcal{L}(D)$ of an $\mathbb{F}_q$-rational divisor D is the $\mathbb{F}_q$-vector space

$$\mathcal{L}(D) = \{f \in \mathbb{F}_q(\mathcal{X}) \mid (f) + D \geq 0\} \cup \{0\}.$$

where $(f) = (f)_0 - (f)_\infty$ denotes the principal divisor of f; here, $(f)_0$ and $(f)_\infty$ are respectively the zero divisor and the pole divisor of f. The $\mathbb{F}_q$-dimension of $\mathcal{L}(D)$ is denoted by $\ell(D)$. It is known that $\mathcal{L}(D)$ is a finite dimensional $\mathbb{F}_q$-vector space and the exact dimension can be computed using the Riemann-Roch theorem. The $\mathbb{F}_q$-dimension of $\mathcal{L}(D)$ is denoted by $\ell(D)$.

Consider now the divisor $D = \sum_{P \in S} P$, $S = \{P_1, \ldots, P_n\} \subsetneq \mathcal{X}(\mathbb{F}_q)$, where all the P's have valuation one. Let G be another $\mathbb{F}_q$-rational divisor such that $\mathrm{supp}(G) \cap \mathrm{supp}(D) = \emptyset$. Consider the evaluation map

$$\mathrm{ev} : \mathcal{L}(G) \to (\mathbb{F}_q)^n \quad , \quad \mathrm{ev}(f) = (f(P_1), \ldots, f(P_n)).$$

This map is $\mathbb{F}_q$-linear and it is injective if $n > \deg(G)$.

The AG-code $C_{\mathcal{L}}(D, G)$ associated with the divisors D and G is then defined as $\mathrm{ev}(\mathcal{L}(G))$. It is well known that $\ell(G) > \ell(G - D)$ and that $C_{\mathcal{L}}(D, G)$ is an $[n, \ell(G) - \ell(G - D), d]_q$ code, where $d \geq d^* = n - \deg(G)$, and d^* is the so called *designed minimum distance* of the code.

3 Intersections between $\mathcal{X}$ and a curve $y = A(x)$ of degree h

Our aim is to find out the intersection over $\mathbb{F}_{q^3}$ of $\mathcal{X}$ with the curve defined by the polynomial $y = A(x)$ of degree h, so $A(x) = A_h x^h + \cdots + A_0$, where $A_h \neq 0$ and $A_i \in \mathbb{F}_{q^r}$. More precisely, given two curves $\mathcal{X}$ and $\mathcal{Y}$ lying in the affine plane $\mathbb{A}^2(\mathbb{F}_{q^r})$ we call *planar intersection* (or simply intersection) the number of points in $\mathbb{A}^2(\mathbb{F}_{q^r})$ that lie in both curves, disregarding multiplicity. Substituting $y = A(x)$ in the equation of the norm-trace curve, we get, by the linearity of T,

$$\mathrm{N}(x) = \mathrm{T}(A_h x^h) + \cdots + \mathrm{T}(A_1 x) + \mathrm{T}(A_0).$$

Given a basis $\mathcal{B} = \{w_0, \ldots, w_{r-1}\}$ of $\mathbb{F}_{q^r}$ over $\mathbb{F}_q$, we know that there is a vector space isomorphism $\Phi_{\mathcal{B}} : (\mathbb{F}_q)^r \to \mathbb{F}_{q^r}$ such that $\Phi_{\mathcal{B}}(s_0, \ldots, s_{r-1}) = \sum_{i=0}^{r-1} s_i w_i$.

The maps $\mathrm{N}, \mathrm{T} : \mathbb{F}_{q^r} \to \mathbb{F}_q$ can be seen as maps from $(\mathbb{F}_q)^r$ to $\mathbb{F}_q$, identifying $\widetilde{\mathrm{N}} = \mathrm{N} \circ \Phi_{\mathcal{B}}$ and $\widetilde{\mathrm{T}} = \mathrm{T} \circ \Phi_{\mathcal{B}}$ with N and T. Also, we can consider $\mathrm{T}_i := \mathrm{T}(A_i x^i)$ and $\widetilde{\mathrm{T}}_i := \mathrm{T}_i \circ \Phi_{\mathcal{B}}$, $1 \leq i \leq h$. From now on, we will take as $\mathcal{B}$ a normal basis, i.e. a basis $\mathcal{B} = \{\alpha, \alpha^q, \ldots, \alpha^{q^{r-1}}\}$, for some $\alpha \in \mathbb{F}_{q^3}$. We know that such a basis exists, see [17, Theorem 2.35]. A simple manipulation shows that $\widetilde{\mathrm{N}}$ and $\widetilde{\mathrm{T}}_i$ are homogeneous polynomials of degree respectively r and i in $\mathbb{F}_q[x_0, \ldots, x_{r-1}]$. Therefore

$$\widetilde{\mathrm{N}}(x_0, \ldots, x_{r-1}) = \widetilde{\mathrm{T}}_h(x_0, \ldots, x_{r-1}) + \cdots + \widetilde{\mathrm{T}}_1(x_0, \ldots, x_{r-1}) + D \tag{2}$$

which is the equation of a hypersurface of $\mathbb{A}^r(\overline{\mathbb{F}}_q)$, where $D = \mathrm{T}(A_0)$. Notice that the LHS has degree r, while the RHS has degree h.

4 Case $r = 3$ and $h = 2$

We are interested in this case to find the number of possible intersections between the norm-trace curve and the parabolas. By parabola we mean a curve $y = Ax^2 + Bx + C$, $A, B, C \in \mathbb{F}_{q^3}$ and $A \neq 0$. These numbers help to determine some weights for the corresponding AG code, see Section 6. From now on, $\mathcal{B} = \{\alpha, \alpha^q, \alpha^{q^2}\}$.

Specializing to $y = Ax^2 + Bx + C$, Equation (2) reads

$$\widetilde{\mathrm{N}}(x_0, x_1, x_2) = \widetilde{\mathrm{T}}_2(x_0, x_1, x_2) + \widetilde{\mathrm{T}}_1(x_0, x_1, x_2) + D. \tag{3}$$

The map $\Phi_{\mathcal{B}}^{-1} : \mathbb{F}_{q^3} \to (\mathbb{F}_q)^3$ induces a correspondence between $\mathbb{F}_q[x_0, x_1, x_2]$ and $\mathbb{F}_{q^3}[x]$ such that we can substitute x with $x_0\alpha + x_1\alpha^q + x_2\alpha^{q^2}$ and x^2 with

$$x_0^2\alpha^2 + x_1^2\alpha^{2q} + x_2^2\alpha^{2q^2} + 2x_0x_1\alpha^{q+1} + 2x_0x_2\alpha^{q^2+1} + 2x_1x_2\alpha^{q^2+q}.$$

Using this relation we want to write down the explicit equation of the surface (3) of AG(3, q).

$$\begin{aligned}\widetilde{\mathrm{T}}_1 &= B(x_0\alpha + x_1\alpha^q + x_2\alpha^{q^2}) + B^q(x_0\alpha^q + x_1\alpha^{q^2} + x_2\alpha) + B^{q^2}(x_0\alpha^{q^2} + x_1\alpha + x_2\alpha^q) \\ &= x_0\mathrm{T}(\alpha B) + x_1\mathrm{T}(\alpha B^{q^2}) + x_2\mathrm{T}(\alpha B^q),\end{aligned}$$

$$\begin{aligned}\widetilde{\mathrm{T}}_2 =& A(x_0\alpha + x_1\alpha^q + x_2\alpha^{q^2})^2 + A^q(x_0\alpha^q + x_1\alpha^{q^2} + x_2\alpha)^2 + A^{q^2}(x_0\alpha^{q^2} + x_1\alpha + x_2\alpha^q)^2 \\ =& x_0^2\mathrm{T}(A\alpha^2) + x_1^2\mathrm{T}(A\alpha^{2q}) + x_2^2\mathrm{T}(A\alpha^{2q^2}) + 2x_0x_1\mathrm{T}(A\alpha^{q+1}) + 2x_0x_2\mathrm{T}(A\alpha^{q^2+1}) + 2x_1x_2\mathrm{T}(A\alpha^{q^2+q}),\end{aligned}$$

$$\begin{aligned}\widetilde{\mathrm{N}} =&(x_0\alpha^{q^2}+x_1\alpha+x_2\alpha^q)(x_0\alpha^q+x_1\alpha^{q^2}+x_2\alpha)(x_0\alpha+x_1\alpha^q+x_2\alpha^{q^2})\\ =&(x_0^3+x_1^3+x_2^3)\mathrm{N}(\alpha)+(x_0^2x_1+x_1^2x_2+x_2^2x_0)\mathrm{T}(\alpha^{q+2})+(x_0^2x_2+x_1^2x_0+x_2^2x_1)\mathrm{T}(\alpha^{2q+1})\\ &+x_0x_1x_2(3\mathrm{N}(\alpha)+\mathrm{T}(\alpha^3)).\end{aligned}$$

Therefore (3) reads

$$\begin{aligned}0=&-(x_0^3+x_1^3+x_2^3)\mathrm{N}(\alpha)-(x_0^2x_1+x_1^2x_2+x_2^2x_0)\mathrm{T}(\alpha^{q+2})-(x_0^2x_2+x_1^2x_0+x_2^2x_1)\mathrm{T}(\alpha^{2q+1})\\ &-x_0x_1x_2(3\mathrm{N}(\alpha)+\mathrm{T}(\alpha^3))+x_0^2\mathrm{T}(A\alpha^2)+x_1^2\mathrm{T}(A\alpha^{2q})+x_2^2\mathrm{T}(A\alpha^{2q^2})+2x_0x_1\mathrm{T}(A\alpha^{q+1})\\ &+2x_0x_2\mathrm{T}(A\alpha^{q^2+1})+2x_1x_2\mathrm{T}(A\alpha^{q^2+q})+x_0\mathrm{T}(\alpha B)+x_1\mathrm{T}(\alpha B^{q^2})+x_2\mathrm{T}(\alpha B^q)+D.\end{aligned}\tag{4}$$

Denote by $\mathcal{S}_1$ the surface defined by the polynomial above. Note that $\mathcal{S}_1$ is defined over $\mathbb{F}_q$. For a given surface, let $\mathcal{X}(\mathbb{F}_q)$ be the set of its $\mathbb{F}_q$-rational points.

Remark 4.1. *By construction, the $\mathbb{F}_q$-rational points of $\mathcal{S}_1$, i.e. the points in $\mathcal{S}_1(\mathbb{F}_q)$, correspond to the intersections in $\mathbb{A}^2(\mathbb{F}_{q^3})$ between the norm-trace curve and the parabola $y=Ax^2+Bx+C$. This happens because (4) comes from a sequence of manipulations that started with $\mathrm{N}(x)=\mathrm{Tr}(Ax^2+Bx+C)$, i.e. there exists an $x\in\mathbb{F}_{q^3}$ such that $\mathrm{N}(x)=\mathrm{Tr}(Ax^2+Bx+C)$ if and only if there exist $(x_0,x_1,x_2)\in(\mathbb{F}_q)^3$ that satisfies (4) and $x=x_0\alpha+x_1\alpha^q+x_2\alpha^{q^2}$.*

Equation (4) can be also written as

$$\begin{aligned}0=&-(x_0\alpha+x_1\alpha^q+x_2\alpha^{q^2})(x_0\alpha^q+x_1\alpha^{q^2}+x_2\alpha)(x_0\alpha^{q^2}+x_1\alpha+x_2\alpha^q)+A(x_0\alpha+x_1\alpha^q+x_2\alpha^{q^2})^2\\ &+A^q(x_0\alpha^q+x_1\alpha^{q^2}+x_2\alpha)^2+A^{q^2}(x_0\alpha^{q^2}+x_1\alpha+x_2\alpha^q)^2+B(x_0\alpha+x_1\alpha^q+x_2\alpha^{q^2})\\ &+B^q(x_0\alpha^q+x_1\alpha^{q^2}+x_2\alpha)+B^{q^2}(x_0\alpha^{q^2}+x_1\alpha+x_2\alpha^q)+D.\end{aligned}$$

Consider the non-singular matrix (since we are dealing with three linearly independent elements, see [17, Corollary 2.38])

$$M=\begin{pmatrix}\alpha & \alpha^q & \alpha^{q^2}\\ \alpha^q & \alpha^{q^2} & \alpha\\ \alpha^{q^2} & \alpha & \alpha^q\end{pmatrix}$$

and the affine change of variables in $\mathbb{A}^3$ defined by $\psi(x_0,x_1,x_2)=M(x_0,x_1,x_2)^t$. Let $\mathcal{S}_2$ be the corresponding surface obtained from $\mathcal{S}_1$. Then $\mathcal{S}_2$ is defined over $\mathbb{F}_{q^3}$, and has equation

$$X_0X_1X_2=AX_0^2+A^qX_1^2+A^{q^2}X_2^2+BX_0+B^qX_1+B^{q^2}X_2+D.\tag{5}$$

Remark 4.2. *Clearly, $\mathbb{F}_q$-rational points of $\mathcal{S}_1$ are mapped to $\mathbb{F}_{q^3}$-rational points of $\mathcal{S}_2$ of the form $(\beta, \beta^q, \beta^{q^2})$, $\beta \in \mathbb{F}_{q^3}$, and viceversa. Moreover, ψ preserves number and degree of any absolutely irreducible component of $\mathcal{S}_1$ and its singularities.*

Proposition 4.3. *$\mathcal{S}_1$ is an absolutely irreducible cubic surface.*

Proof. By Remark 4.2 it is sufficient to prove that $\mathcal{S}_2$ is absolutely irreducible. We proceed by contradiction. If $\mathcal{S}_2$ is reducible, since its degree is three, then it must contain a plane. In this case we would have

$$q(X_0, X_1, X_2)(k_0X_0 + k_1X_1 + k_2X_2 + k_3) = X_0X_1X_2 - AX_0^2 - A^qX_1^2 - A^{q^2}X_2^2 - BX_0 - B^qX_1 - B^{q^2}X_2 - D \quad (6)$$

where $q(x_0, x_1, x_2)$ is the equation of a quadric surface, $k_j \in \overline{\mathbb{F}}_q$, $j \in \{0, \ldots, 3\}$, and at least one of k_0, k_1, k_2 is nonzero.

Consider the intersections of $\mathcal{S}_2$ with the plane at the infinity, then

$$Q(X_0, X_1, X_2)(k_0X_0 + k_1X_1 + k_2X_2) = X_0X_1X_2$$

where $Q(X_0, X_1, X_2)$ is the polynomial given by the degree 2 terms of $q(X_0, X_1, X_2)$. This expression implies that two among k_0, k_1, k_2 have to be zero, and then the plane has equation $k_iX_i + k_3 = 0$ for $i \in \{0, 1, 2\}$. Suppose, whitout loss of generality that $i = 0$, then Equation (6) reads

$$q(X_0, X_1, X_2)(X_0 + k) = X_0X_1X_2 - AX_0^2 - A^qX_1^2 - A^{q^2}X_2^2 - BX_0 - B^qX_1 - B^{q^2}X_2 - D$$

for a given $k \in \overline{\mathbb{F}}_q$.

Applying the identity principle for polynomials, we obtain that $q(X_0, X_1, X_2) = X_1X_2 + h_0X_0 + h_1X_1 + h_2X_2 + h_3$, where $h_i \in \overline{\mathbb{F}}_q$, $i \in \{0, \ldots, 3\}$. At this point Equation (6) becomes

$$(X_1X_2 + h_0X_0 + h_1X_1 + h_2X_2 + h_3)(k_0X_0 + k_3) = X_0X_1X_2 - AX_0^2 - A^qX_1^2 - A^{q^2}X_2^2 - BX_0 - B^qX_1 - B^{q^2}X_2 - D$$

and since $A^q \neq 0$ this cannot happen.

□

What we want to do now is to estimate the number of $\mathbb{F}_q$-rational points of $\mathcal{S}_1$. Since they correspond to the intersections between $\mathcal{X}$ and $y = Ax^2 + Bx + C$, by applying the Bézout theorem we get that

$$|\mathcal{S}_1(\mathbb{F}_q)| \leq 2(q^2 + q + 1).$$

This bound can be improved, as we will see. A better estimate can be obtained using the Lang-Weil bound.

Theorem 4.4 ([16]). *Given nonnegative integers n, d and r, with $d > 0$, there is a positive constant $A(n, d, r)$ such that for every finite field $\mathbb{F}_q$, and every irreducible subvariety $\mathcal{X} \subseteq \mathbb{P}^n(\mathbb{F}_q)$ of dimension r and degree d, we have*

$$||\mathcal{X}(\mathbb{F}_q)| - q^r| \leq (d-1)(d-2)q^{r-\frac{1}{2}} + A(n,d,r)q^{r-1}.$$

Corollary 4.5. *The number of $\mathbb{F}_q$-rational points on the surface $\mathcal{S}_1(\mathbb{F}_q)$ is bounded by*

$$q^2 + 2q^{\frac{3}{2}} + A(3,3,2)q.$$

This bound improves Bézout's Theorem. Also, other theoretical estimates are known; see [6]. In what follows we will provide a bound of the type

$$\mathcal{S}_1(\mathbb{F}_q) \leq q^2 + \eta q + \mu$$

where $\mu < q$ and η is upper bounded by a constant (independent from q and μ). Experimentally we found the following

Fact 4.6. *For $q \in \{2, \ldots, 29\}$, $|\eta| \leq 2$ and $\mu = 1$.*

Conjecture 4.7. *$|\eta| \leq 2$ and $\mu = 1$ for all q.*

Recall some previous results

Theorem 4.8 ([18], Theorem 27.1). *Let $\mathcal{S}$ be a cubic surface over $\mathbb{F}_q$. If $\mathcal{S}$ is birationally trivial (i.e. to allow a $\mathbb{F}_q$-birational map to $\mathbb{P}^2(\mathbb{F}_q)$), then*

$$|S(\mathbb{F}_q)| \equiv 1 \mod q.$$

In the case in which S_1 is smooth we also know the possible values for $|S_1(\mathbb{F}_q)|$.

Theorem 4.9 ([18], Theorem 23.1). *Let $\mathcal{S}$ be a smooth irreducible cubic surface over $\mathbb{F}_q$, then the number of points of $\mathcal{S}(\mathbb{F}_q)$ is exactly*

$$|\mathcal{S}(\mathbb{F}_q)| = q^2 + \eta q + 1$$

where $\eta \in \{-2, -1, 0, 1, 2, 3, 4, 5, 7\}$.

In view of Theorem 4.9, we consider separately the cases $\mathcal{S}_1$ smooth and $\mathcal{S}_1$ singular.

5 Singular case

From now on we investigate when $\mathcal{S}_1$ is singular. We start by observing that the possible singular points can only be double points, since $\mathcal{S}_1$ is a cubic irreducible surface. Moreover, recalling that an isolated singularity P_s means that there exists a neighbourhood containing only P_s as singular point, we will see that $\mathcal{S}_2$ has only isolated singularities. This happens beacuse the ideal defined by its equation and the partial derivatives is zero-dimensional (as it is possible to see in the proof of Proposition 5.13). In this context the following result is very helpful.

Theorem 5.1 ([7]). *Let $\mathcal{S} \subset \mathbb{P}^3(\mathbb{K})$ be a singular irreducible cubic surface defined on the field $\mathbb{K}$. Let $\bar{\mathcal{S}} = \mathcal{S}(\overline{\mathbb{K}})$ be the surface defined by $\mathcal{S}$ over $\overline{\mathbb{K}}$, the algebraic closure of $\mathbb{K}$. Let δ be the number of isolated double points of $\bar{\mathcal{S}}$. Then $\delta \leq 4$ and $\mathcal{S}$ is birationally equivalent (over $\mathbb{K}$) to*

(i) $\mathbb{P}^2(\mathbb{K})$ if $\delta = 1, 4$;

(ii) a smooth Del Pezzo surface of degree 4 if $\delta = 2$;

(iii) a smooth Del Pezzo surface of degree 6 if $\delta = 3$.

Recall that a smooth Del Pezzo surface is a smooth projective surface V whose anticanonical class is ample. Many arithmetic properties of these surfaces were investigated by Manin; see [18].

What we want to do now is to find a bound of type $q^2 + \eta q + \mu$ for the four possible cases of singularities ($\delta = 1, 2, 3, 4$).

Clearly the affine singular points on $\mathcal{S}_2$ correspond to the solutions of

$$\begin{cases} X_0X_1X_2 = AX_0^2 + A^qX_1^2 + A^{q^2}X_2^2 + BX_0 + B^qX_1 + B^{q^2}X_2 + D \\ X_1X_2 = 2AX_0 + B \\ X_0X_2 = 2A^qX_1 + B^q \\ X_0X_1 = 2A^{q^2}X_2 + B^{q^2} \end{cases} \tag{7}$$

Remark 5.2. *$\mathcal{S}_2$ has no singular point at the infinity.*

Proof. A straightforward computation shows that the singular points at the infinity of $\mathcal{S}_2$ satisfy the following system of equations

$$\begin{cases} X_0X_1X_2 = 0 \\ X_1X_2 = 0 \\ X_0X_2 = 0 \\ X_0X_1 = 0 \\ AX_0^2 + A^qX_1^2 + A^{q^2}X_2^2 = 0 \end{cases}$$

which admits only $(0:0:0:0)$ as solution, which is not a point of the projective space. □

Remark 5.3. *Since $\mathcal{S}_1$ is defined over $\mathbb{F}_q$ if $P \in \mathcal{S}_1(\mathbb{F}_q)$ is a singular point then its conjugates with respect to the Frobenius automorphism are also singular.*

Remark 5.4. *Notice also that if a singular point of $\mathcal{S}_2$ is $\mathbb{F}_{q^6}$-rational the corresponding singularity of $\mathcal{S}_1$ will be $\mathbb{F}_{q^2}$-rational since $(x_0\alpha + x_1\alpha^q + x_2\alpha^{q^2})^{q^6} = (x_0\alpha + x_1\alpha^q + x_2\alpha^{q^2})^{q^2}$.*

Before considering the classification of the four cases arising from different values of δ, we need to examine separately the case $B = 0$, which turns out ot to be special.

5.1 Case B=0

In this case the singularities of the surface correspond to the solutions of

$$\begin{cases} X_0X_1X_2 = AX_0^2 + A^qX_1^2 + A^{q^2}X_2^2 + D \\ X_1X_2 = 2AX_0 \\ X_0X_2 = 2A^qX_1 \\ X_0X_1 = 2A^{q^2}X_1 \end{cases} \tag{8}$$

A direct computation leads to the fact that if $(\bar{x}_0, \bar{x}_1, \bar{x}_2) \neq (0,0,0)$ is a singular point, then each $\bar{x}_i$ is different from zero.

Proposition 5.5. *The only possible singularities for the case $B = 0$ are described in the following list:*

(i) if $D = 0$ then, for any q, $\mathcal{S}_2$ admits only $P = (0,0,0)$ as singular point;

(ii) if $D \neq 0$ and q is odd then $\delta = 4$ and the singular points are given by $(\gamma, \gamma^q, \gamma^{q^2})$, $(\gamma, -\gamma^q, -\gamma^{q^2})$, $(-\gamma, \gamma^q, -\gamma^{q^2})$, $(-\gamma, -\gamma^q, \gamma^{q^2})$, where $\gamma = 2A^{\frac{q^2+q}{2}}$.

Proof. Direct computations show that (i) comes from Equation (8), so we are left with the case q odd and $(0,0,0)$ not singular. Substituting the derivatives into the equation that defines the surface we get

$$\begin{cases} -AX_0^2 + A^qX_1^2 + A^{q^2}X_2^2 + D = 0 \\ AX_0^2 - A^qX_1^2 + A^{q^2}X_2^2 + D = 0 \\ AX_0^2 + A^qX_1^2 - A^{q^2}X_2^2 + D = 0. \end{cases}$$

Summing pairwise the equations gives us

$$\begin{cases} 2AX_0^2 + 2D = 0 \\ 2A^qX_1^2 + 2D = 0 \\ 2A^{q^2}X_2^2 + 2D = 0 \end{cases}$$

and, since q is odd and $A \neq 0$

$$\begin{cases} X_0^2 = -\frac{D}{A} \\ X_1^2 = -\frac{D}{A^q} \\ X_2^2 = -\frac{D}{A^{q^2}} \end{cases} \tag{9}$$

The fact that $\beta \in \mathbb{F}_q$ is a square if and only if β^q is a square implies that all the equations of (9) are solvable if and only if the first one is. Therefore (9) is solvable if and only if $-\frac{D}{A}$ is a square of $\mathbb{F}_{q^3}$, but this is always true since $-\frac{D}{A} = A^{q^2+q}$ has is an even power of A. From the equation of the surface it follows that $\mathcal{S}_2$ has four singularities of the form $(\gamma, \gamma^q, \gamma^{q^2})$, $(\gamma, -\gamma^q, -\gamma^{q^2})$, $(-\gamma, \gamma^q, -\gamma^{q^2})$, $(-\gamma, -\gamma^q, \gamma^{q^2})$, where $\gamma = 2A^{\frac{q^2+q}{2}}$.

□

Remark 5.6. *Notice that in case $D \neq 0$ and q odd, the four singular points cannot be all distinct conjugates with respect to the Frobenius automorphism. This comes from the explicit representation that was given above, and from the fact that if $\gamma^q = \pm\gamma$ then each point can have at most one different conjugate.*

5.2 One singular point

From now on we can consider $B \neq 0$. From Remark 5.3 if $\mathcal{S}_1$ has one singular (double) point P then P has to be $\mathbb{F}_q$-rational, otherwise also its conjugate should be singular. Consider now the sheaf of $\mathbb{F}_q$-rational lines passing through P: each line, not contained in $\mathcal{S}_1(\mathbb{F}_q)$, can intersect $\mathcal{S}_1(\mathbb{F}_q)$ in at most one more point, since P is a double point and $\mathcal{S}_1$ has degree three. So the number of $\mathbb{F}_q$-rational points of $\mathcal{S}_1$ is given by

$$|S_1(\mathbb{F}_q)| \leq q^2 + h(q-1) = q^2 + hq - h$$

where h is the number of lines contained in $\mathcal{S}_1$ and passing through P.

Proposition 5.7. *With the same notation as before we have $h = 0$.*

Proof. We want to give a bound for the maximal number of ($\mathbb{F}_q$-rational) lines contained in $\mathcal{S}_1$ and passing through P. For simplicity we proceed with the computations on $\mathcal{S}_2$, since the number of these lines will be the same. Suppose that the corresponding singular point Q on $\mathcal{S}_2$ has coordinates (a, a^q, a^{q^2}). Then, since it is the only singular point, we have that Q is the only point that satisfies (7). Consider now the sheaf of lines passing through Q, which has parametric equation, for $b \neq 0$

$$\begin{cases} X_0 = bt + a \\ X_1 = b^q t + a^q \\ X_2 = b^{q^2} t + a^{q^2} \end{cases}$$

and after doing the substitution we get that, if the line is contained into $\mathcal{S}_2$,

$$p_3 t^3 + p_2 t^2 + p_1 t$$

has to be the zero polynomial in $\mathbb{F}_q[t]$, where

$$\begin{aligned} p_3 &= b^{q^2+q+1}, \\ p_2 &= -Ab^2 - (Ab^2)^q - (Ab^2)^{q^2} + b^{q+1}a^{q^2} + b^{q^2+1}a^q + b^{q^2+q}a, \\ p_1 &= -2Aab - 2(Aab)^q - 2(Aab)^{q^2} - Bb - (Bb)^q - (Bb)^{q^2} + ba^{q^2+q} + b^q a^{q^2+1} + b^{q^2}a^{q+1}. \end{aligned}$$

From the fact that $p_3 = 0$ we have that $\mathrm{N}(b)$ has to be equal to zero, but this means that b is equal to zero, which is a contradiction. □

Putting together the previous observations we have the following result.

Proposition 5.8. *If $\mathcal{S}_1$ has one singular $\mathbb{F}_q$-rational point then*

$$|S_1(\mathbb{F}_q)| \leq q^2. \tag{10}$$

5.3 Two singular points

Call P_1 and P_2 the two singular points of $\mathcal{S}_1$, from Remark 5.3 there are two possibilities:

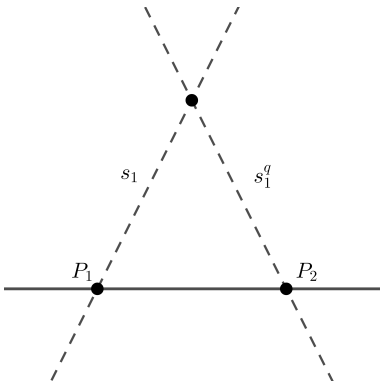
(i) P_1 and P_2 are $\mathbb{F}_q$-rational;

(ii) P_1 and P_2 are $\mathbb{F}_{q^2}$-rational and conjugates.

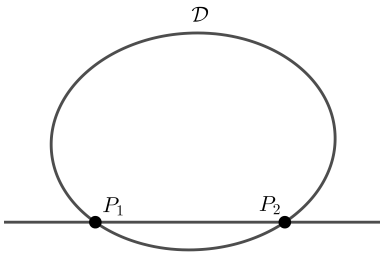
If (i) happens then we can give similar argumentation as in Section 5.2 and get the bound $|S_1(\mathbb{F}_q)| \leq q^2 + q - 1$.

We look for a bound when (ii) happens: call r the line passing through P_1 and P_2, since it fixes the conjugate points then it has to be $\mathbb{F}_q$-rational and moreover this line has to be contained in $\mathcal{S}_1(\mathbb{F}_q)$ since the intersection multiplicity of this line is at least 2 in both P_1 and P_2 and the surface has degree 3. Now consider the pencil of planes passing through r and consider the cubic curve $\mathcal{C}$ defined as intersection between any of these planes and $\mathcal{S}_1$. Clearly $\mathcal{C}$ is reducible and there are two possible situations:

1. $\mathcal{C}$ is completely reducible. In this case $\mathcal{C}$ is the product of three lines contained in the surface. Call s and s' the two lines different from r: s and s' cannot be $\mathbb{F}_q$-rational since they do not fix the conjugates, so they are $\mathbb{F}_{q^2}$-rational. From the fact that they are contained in $\mathcal{S}_1$ and they pass through conjugate points we have that $s' = s^q$. From this fact we have that the number of $\mathbb{F}_q$-rational points on $\mathcal{C} \setminus r$ is 1 and that point is $s \cap s'$.



2. $\mathcal{C}$ is the product of r and an irreducible conic $\mathcal{D}$ contained in the surface and it contains exactly q points, see [14, Lemma 7.2.3]. In this case the number of $\mathbb{F}_q$ rational points of $\mathcal{D}$ not contained in r is exactly $q - 2$.



From the analysis of the two possible cases, recalling that the maximum number of lines contained in a cubic surface is 27 (see [18, Chapter IV]), the first situation can happen at most in 13 cases, and so we have:

$$q + (q-13)(q-2) + 13 \leq |S_1(\mathbb{F}_q)| \leq q(q-2) + q$$

Putting together the previous observations we have the following result.

Proposition 5.9. *If $\mathcal{S}_1$ has two singular $\mathbb{F}_{q^2}$-rational conjugate points then*

$$q^2 - 14q + 39 \leq |S_1(\mathbb{F}_q)| \leq q^2 - q. \tag{11}$$

5.4 Three singular points

Call P_1, P_2 and P_3 the singular points of $\mathcal{S}_1$, from Remark 5.3 we have the following configurations:

(i) At least one among P_1, P_2 and P_3 is $\mathbb{F}_q$-rational;

(ii) P_1, P_2 and P_3 are $\mathbb{F}_{q^3}$-rational and conjugates.

If (i) happens then we can give similar argumentation as in Section 5.2 and get the bound $|S_1(\mathbb{F}_q)| \leq q^2 + 2q - 2$.

We start with observing that the three points cannot be collinear, which comes directly from the following proposition.

Proposition 5.10. *Let $\mathcal{C}$ be a cubic curve such that it has three double points. Then $\mathcal{C}$ is completely reducible and splits in the product of three lines, each passing through a pair of its singular points.*

Proof. Direct consequence of Bézout's theorem. □

In order to get an estimation of $|\mathcal{S}_1(\mathbb{F}_q)|$ for (ii) we change the model of the surface as the following proposition suggests.

Proposition 5.11. *Let $\mathcal{S}$ be a cubic surface over $\mathbb{P}^3(\mathbb{F}_q)$, considered with projective coordinates $[r_0 : r_1 : r_2 : T]$, and such that it has exactly three conjugates $\mathbb{F}_{q^3}$-rational double points, namely P_1, P_2 and P_3. Then $\mathcal{S}$ is projectively equivalent to the surface having affine equation, for certain $\beta, \gamma \in \mathbb{F}_{q^3}$*

$$r_0r_1r_2 + \beta r_0r_1 + \beta^q r_1r_2 + \beta^{q^2} r_0r_2 + \gamma r_0 + \gamma^q r_1 + \gamma^{q^2} r_2 = 0.$$

Proof. Up to a change of projective frame we can consider the following situation

- The plane passing trough the three points is the plane at the infinity $T = 0$ and the triangle of lines through them in that plane is given by r_0, r_1 and r_2;
- $\mathcal{O} = (0 : 0 : 0 : 1) \in \mathcal{S}$.

From these choices we obtain the following equation for the surface $\mathcal{S}$

$$r_0r_1r_2 + T(\alpha_0 r_0^2 + \alpha_1 r_1^2 + \alpha_2 r_2^2 + \beta_0 r_0r_1 + \beta_1 r_1r_2 + \beta_2 r_0r_2) + T^2(\gamma_0 r_0 + \gamma_1 r_1 + \gamma_2 r_2) = 0$$

where $\alpha_i, \beta_i, \gamma_i \in \mathbb{F}_{q^3}$ for $i \in \{0, 1, 2\}$. From the fact that P_1, P_2 and P_3 are conjugates it follows that r_0, r_1 and r_2 are conjugates and then we get that $\alpha_1 = \alpha_0^q$, $\alpha_2 = \alpha_0^{q^2}$, $\beta_1 = \beta_0^q$, $\beta_2 = \beta_0^{q^2}$, $\gamma_1 = \gamma_0^q$ and $\gamma_2 = \gamma_0^{q^2}$. Consider now the plane π passing trough P_1, P_2 and $\mathcal{O}$. Without loss of generality, P_1 is the singular point satisfying $T = r_1 = r_2 = 0$, then its coordinates will be $P_1 = (p_1, p_2, p_3, 0)$. Consider now the line, namely s passing through P_1 and $\mathcal{O}$. A general point on that line has coordinates $P_{\lambda,\mu} = (\lambda p_0, \lambda p_1, \lambda p_2, \mu)$. Substituting the coordinates of $P_{\lambda,\mu}$ into the equation of $\mathcal{S}$ we obtain

$$0 = \alpha_0 \lambda r_0^2(P_{\lambda,\mu}) + \beta_0 \lambda^2 r_0(P_{\lambda,\mu}) = \lambda(\alpha_0 r_0^2(P_{\lambda,\mu}) + \beta_0 \lambda r_0(P_{\lambda,\mu})).$$

Now since $r_0(P_1) \neq 0$ and we want $(0, \mu)$ as double solution then $\alpha_0 = 0$. Iterating this process the equation of the surface becomes

$$r_0r_1r_2 + T(\beta_0 r_0r_1 + \beta_0^q r_1r_2 + \beta_0^{q^2} r_0r_2) + T^2(\gamma_0 r_0 + \gamma_0^q r_1 + \gamma_0^{q^2} r_2) = 0.$$

□

We want to reduce the problem of counting the points in the form $(\alpha, \alpha^q, \alpha^{q^2})$ on the cubic surface to the problem of counting the points in the same form on a certain quadric. To achieve the result we apply the Cremona transform, call

$$z_1 := \frac{1}{r_1} \quad z_2 := \frac{1}{r_2} \quad z_3 := \frac{1}{r_3},$$

dividing the equation of the surface by $r_1 r_2 r_3$ we obtain

$$\mathcal{Q} : \beta z_3 + \beta^q z_1 + \beta^{q^2} z_2 + \gamma z_2 z_3 + \gamma^q z_1 z_3 + \gamma^{q^2} z_1 z_2 - 1 = 0.$$

Note that if $\gamma = 0$ then $\mathcal{Q}$ collapse to a plane.

Proposition 5.12. *The quadric surface $\mathcal{Q}$ is absolutely irreducible.*

Proof. If $\gamma = 0$ there is nothing to prove, since $\mathcal{Q}$ is a plane. Suppose $\gamma \neq 0$ and that $\mathcal{Q}$ splits in the product of two planes π_1 and π_2, then

$$\beta z_3 + \beta^q z_1 + \beta^{q^2} z_2 + \gamma z_2 z_3 + \gamma^q z_1 z_3 + \gamma^{q^2} z_1 z_2 - 1 = (a_1 z_1 + a_2 z_2 + a_3 z_3 + a_4)(d_1 z_1 + d_2 z_2 + d_3 z_3 + d_4).$$

From the identity principles of polynomials we get that $a_1 d_1 = a_2 d_2 = a_3 d_3 = 0$ Without loss of generality we can consider $a_1 = a_2 = d_3 = 0$ and then the equation becomes

$$\beta z_3 + \beta^q z_1 + \beta^{q^2} z_2 + \gamma z_2 z_3 + \gamma^q z_1 z_3 + \gamma^{q^2} z_1 z_2 - 1 = (a_3 z_3 + a_4)(d_1 z_1 + d_2 z_2 + d_4)$$

and this cannot happen since in the right hand side of this equality we do not have the term $z_1 z_2$. □

We want to count the points on the quadric $\mathcal{Q}$ in the form $(\delta, \delta^q, \delta^{q^2})$, where $\delta \in \mathbb{F}_{q^3}$. Writing down δ on the normal basis $\mathcal{B}$ we get $\delta = w_1\alpha + w_2\alpha^q + w_3\alpha^{q^2}$. Taking w_1, w_2 and w_3 as a set of variables (on $\mathbb{F}_q$) we obtain a $\mathbb{F}_q$-rational quadric surface and its $\mathbb{F}_q$-rational points are in one-to-one correspondence with the searched ones.

$$\beta(w_1\alpha^{q^2} + w_2\alpha + w_3\alpha^q) + \beta^q(w_1\alpha + w_2\alpha^q + w_3\alpha^{q^2}) + \beta^{q^2}(w_1\alpha^q + w_2\alpha^{q^2} + w_3\alpha) +$$
$$\gamma(w_1\alpha + w_2\alpha^q + w_3\alpha^{q^2})(w_1\alpha^q + w_2\alpha^{q^2} + w_3\alpha) + \gamma^q(w_1\alpha^{q^2} + w_2\alpha + w_3\alpha^q)(w_1\alpha^q + w_2\alpha^{q^2} + w_3\alpha) +$$
$$\gamma^{q^2}(w_1\alpha^{q^2} + w_2\alpha + w_3\alpha^q)(w_1\alpha + w_2\alpha^q + w_3\alpha^{q^2}) - 1 = 0.$$

The points we were looking for of the first surface are in one-to-one correspondence with the $\mathbb{F}_q$-rational points on the quadric surface above. It is widely known (see [13, Section 15.3]) that, in this case

$$|S_1(\mathbb{F}_q)| = q^2 + \eta q + 1, \quad \eta \in \{0, 1, 2\} \tag{12}$$

since the quadric surface $\mathcal{Q}$ is irreducible.

5.5 Four singular points

Call P_1, P_2, P_3 and P_4 the singular points of $\mathcal{S}_1$, applying Remark 5.3 we have the following possibilities:

(i) At least one among P_1, P_2, P_3 and P_4 is $\mathbb{F}_q$-rational;

(ii) There are two couples of $\mathbb{F}_{q^2}$-rational and conjugates singular points.

(iii) P_1, P_2, P_3 and P_4 are $\mathbb{F}_{q^4}$-rational and conjugates.

If (i) or (ii) hold then we have already found out a good bound before respectively $|S_1(\mathbb{F}_q)| \leq q^2 + 3q - 3$ and $|S_1(\mathbb{F}_q)| \leq q^2$, the last thing we have to do is show that (iii) never holds.

Proposition 5.13. *Case (iii) never holds.*

Proof. In order to solve this problem we use a multivariate approach, calculating the elimination ideal with respect to all the variables less one. Consider the equations in (7): it is clear that, given X_1 and X_2, the value of X_0 is uniquely determined. For this reason we proceed with eliminating the variables X_0 and X_1 and we obtain the elimination ideal $I_{x_0,x_1} = \langle p_1, p_2 \rangle$, where

$$\begin{aligned} p_1(X_1) =& 2X_1^5 A^q + X_1^4 B^q - 16X_1^3 A^{q^2+q+1} - 8X_1^2 A^{q^2+1} B^q - X_1^2 B^{q^2+1} + 32X_1 A 2q^2 + q + 2 \\ & - 2X_1 A B^{2q^2} - 2X_1 A^{q^2} B^2 + 16A^{2q^2+2} B^q - 4A^{q^2+1} B^{q^2+1} \\ p_2(X_1) =& (X_1^2 - 4A^{q^2+1})(X_1^4 A^q + X_1^3 B^q - 4X_1^2 A^{q^2+q+1} + X_1^2 D - 4X_1 A^{q^2+1} B^q \\ & + x1 B^{q^2+1} - 4A^{q^2+1} D + A B^{2q^2} + A^{q^2} B^2). \end{aligned}$$

On the other hand, if we prooced eliminating the variables X_0 and X_1 we get the elimination ideal $J_{x_0,x_2} = \langle q_1, q_2 \rangle$, where $q_1 = p_1(X_2)^q$ and $q_2 = p_2(X_2)^q$. The fact that the two ideals are generated by conjugate polynomials will continue to be true after symmetric annihilation of some of their terms. After further computations using the software MAGMA, which can be completely seen in [5], we get that one of the generators of I_{x_1,x_2} is a polynomial of degree lower or equal to two, namely $f(X_1)$, and one of the generators of J_{x_0,x_2} is $f(X_2)^q$. From this fact we get that the singularities of $\mathcal{S}_2$ are at most four and if this value is achieved then they belong (at most) to the field $\mathbb{F}_{q^6}$, which means that the singularities of $\mathcal{S}_1$ are at most in the field $\mathbb{F}_{q^2}$. □

6 Case $r = 3$ and $h = 3$

Consider the case of the intersection over $\mathbb{F}_{q^3}$ between $\mathcal{X}$ and the curves $y = Ax^3 + Bx^2 + Cx + D$, $A, B, C, D \in \mathbb{F}_{q^3}$ and $A \neq 0$. After doing similar computations to those done for the case $r = 3$ and $h = 2$ we arrive at an equation of a cubic surface $\widehat{\mathcal{S}}_1 = \widehat{\mathcal{S}}_1(\overline{\mathbb{F}}_q)$ defined over $\mathbb{F}_q$, affinely equivalent to a surface $\widehat{\mathcal{S}}_2 = \widehat{\mathcal{S}}_2(\overline{\mathbb{F}}_q)$ defined over $\mathbb{F}_{q^3}$, having equation

$$X_0X_1X_2 = AX_0^3 + A^qX_1^3 + A^{q^2}X_2^3 + BX_0^2 + B^qX_1^2 + B^{q^2}X_2^2 + CX_0 + C^qX_1 + C^{q^2}X_2 + E$$

where $E = \mathrm{T}(D)$. In this more general case $\widehat{\mathcal{S}}_1$ may be reducible, which can possibly increase the number of $\mathbb{F}_q$-rational points of $\widehat{\mathcal{S}}_1$, but on the other hand the reasonings done for $r = 3$ and $h = 2$ can be completely extended if $\widehat{\mathcal{S}}_1$ is irreducible, so we claim the following result.

Theorem 6.1. *Let $r = h = 3$ and consider the $\mathbb{F}_q$-rational cubic surface $\widehat{\mathcal{S}}_1$ associated to the intersections between $\mathcal{X}$ and $y = Ax^3 + Bx^2 + Cx + D$. If $\widehat{\mathcal{S}}_1$ is irreducible then*

$$|\widehat{\mathcal{S}}_1| \leq q^2 + 7q + 1.$$

7 AG codes from the Norm-Trace curves

Consider the norm-trace curve over the field $\mathbb{F}_{q^3}$: since $r = 3$, $\mathcal{X}$ has $N = q^{2r-1} = q^5$ $\mathbb{F}_{q^3}$-rational points in $\mathbb{A}^2(\mathbb{F}_{q^3})$. We also know that $\mathcal{L}_{\mathbb{F}_q}(2q^2P_\infty) = \{ay+bx^2+cx+d \,|\, a, b, c, d \in \mathbb{F}_{q^3}\}$. Considering the evaluation map

$$\begin{aligned} \mathrm{ev}: \ \mathcal{L}_{\mathbb{F}_{q^3}}(2q^2P_\infty) &\longrightarrow (\mathbb{F}_{q^3})^{q^5} \\ f = \tilde{a}y + \tilde{b}x^2 + \tilde{c}x + \tilde{d} &\longmapsto (f(P_1), \ldots, f(P_N)) \end{aligned}$$

the associated one-point code will be $C_{\mathcal{L}}(D, 2q^2P_\infty) = \mathrm{ev}(\mathcal{L}_{\mathbb{F}_{q^3}}(2q^2P_\infty))$, where the divisor D is the formal sum of all the q^5-rational affine points of $\mathcal{X}(\mathbb{F}_{q^3})$. The weight of a codeword associated to the evaluation of a function $f \in \mathcal{L}_{\mathbb{F}_{q^3}}(2q^2P_\infty)$ corresponds to

$$\mathrm{w}(\mathrm{ev}(f)) = |\mathcal{X}(\mathbb{F}_{q^3})| - |\{\mathcal{X}(\mathbb{F}_{q^3}) \cap \{\tilde{a}y + \tilde{b}x^2 + \tilde{c}x + \tilde{d} = 0\}\}|.$$

1. If $\tilde{a} = 0$ then we have to study the common zeroes of $\tilde{b}x^2 + \tilde{c}x + \tilde{d}$ and $\mathcal{X}(\mathbb{F}_{q^3})$.

   (a) if $\tilde{b} = \tilde{c} = \tilde{d} = 0$ then $\mathrm{w}(\mathrm{ev}(f)) = 0$;

(b) if $\tilde{b} = \tilde{c} = 0$ and $\tilde{d} \neq 0$ then $\mathrm{w}(\mathrm{ev}(f)) = q^5$;

(c) if $\tilde{b} = 0$ and $\tilde{c} \neq 0$ then $\mathrm{w}(\mathrm{ev}(f)) = q^5 - q^2$;

(d) if $\tilde{c} \neq 0$ and $\tilde{c}^2 - 4\tilde{b}\tilde{d} = 0$ then $\mathrm{w}(\mathrm{ev}(f)) = q^5 - q^2$;

(e) otherwise $\mathrm{w}(\mathrm{ev}(f)) = q^5 - 2q^2$.

2. On the other hand, if $\tilde{a} \neq 0$ then we have to study the common zeroes between $\mathcal{X}(\mathbb{F}_{q^3})$ and $\tilde{a}y + \tilde{b}x^2 + \tilde{c}x + \tilde{d}$.

(a) if $\tilde{b} = \tilde{c} = \tilde{d} = 0$ then $\mathrm{w}(\mathrm{ev}(f)) = q^5 - 1$;

(b) if $\tilde{b} = \tilde{c} = 0$ and $\tilde{d} \neq 0$ then $\mathrm{w}(\mathrm{ev}(f)) = q^5 - q^2$;

(c) if $\tilde{b} = 0$ and $\tilde{c} \neq 0$ then, applying Bézout theorem, we have that $\mathrm{w}(\mathrm{ev}(f)) \geq q^5 - (q^2 + q + 1)$;

(d) otherwise, from what we said previously, $\mathrm{w}(\mathrm{ev}(f)) \geq q^5 - (q^2 + 7q + 1)$.

We can summarize our reasonings in the following result.

Theorem 7.1. *Consider the norm-trace curve $\mathcal{X}$ over the field $\mathbb{F}_{q^3}$, $q \geq 8$, and the AG code $C = C(D, 2q^2 P_\infty)$ arising from $\mathcal{X}$, where $D = \sum_{P \in \mathcal{X}(\mathbb{F}_{q^3}) \setminus P_\infty} P$. Let $\{A_\mathrm{w}\}_{0 \leq \mathrm{w} \leq q^5}$ be the weight distribution of C, then the following results hold*

(i) $A_0 = 1$;

(ii) The minimum distance of C is $q^5 - 2q^2$;

(iii) If $\mathrm{w} > q^5 - 2q^2$ and $A_\mathrm{w} \neq 0$ then $\mathrm{w} \geq q^5 - q^2 - 7q - 1$;

In the cases $q < 8$, i.e. $q = 2, 3, 5, 7$, the complete $\{A_w\}_{w \leq q^5}$ can be determined with a computer and we do not report it here.

Acknowledgements

The authors would like to thank the anonymous referee for their interesting and useful comments which permitted to improve the paper. This research was partially supported by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM). The results showed in this paper are included in M. Bonini's Ph.D. thesis (supervised by the second author and G. Rinaldo).

References

[1] E. Ballico, A. Ravagnani. On the duals of geometric Goppa codes from norm-trace curves. Finite Fields Appl. **20**, 30-39, (2013).

[2] D. Bartoli, M. Bonini, *Minimum weight codewords in dual algebraic-geometric codes from the Giulietti-Korchmáros curve*, Des. Codes Cryptography, to appear (https://doi.org/10.1007/s10623-018-0541-y) (2018).

[3] D. Bartoli, M. Montanucci, G. Zini. *AG codes and AG quantum codes from the GGS curve*, Des. Codes and Cryptography **86**(10), 2315-2344 (2018).

[4] D. Bartoli, M. Montanucci, G. Zini. *Multi point AG codes on the GK maximal curve*, Des. Codes and Cryptography **86**(1), 161-177 (2018).

[5] M. Bonini. Intersections of Algebraic Curves and their link to the weight enumerators of Algebraic-Geometric Codes. Ph.D. Thesis (2019).

[6] T.D. Browning. *The Lang-Weil estimate for cubic hypersurfaces*, Canad. Math. Bull. 56, 500–502 (2013).

[7] D.F. Coray, M.A. Tsfasman. Arithmetic on singular Del Pezzo surfaces. Proceedings of the London Mathematical Society **3** (1), 25-87(1988).

[8] A. Couvreur, *The dual minimum distance of arbitrary-dimensional algebraic–geometric codes*. Journal of Algebra **350**, 84-107 (2012).

[9] G. Donati, N.Durante, G.Korchmáros. On the intersection pattern of a unital and an oval in $PG(2, q^2)$. Finite Fields and Their Applications **15**, 785–795 (2009).

[10] O. Geil,(2003). On codes from norm–trace curves. Finite fields and their Applications **9** (3), 351–371.

[11] V.D. Goppa. Codes on algebraic curves. Dokl. Akad. NAUK SSSR **259**, 1289–1290 (1981).

[12] V.D. Goppa. Algebraic-geometric codes. Izv. Akad. NAUK SSSR **46**, 75–91 (1982).

[13] J.W.P. Hirschfeld, Finite projective spaces of three dimensions. Oxford University Press, 1985.

[14] J.W.P. Hirschfeld Projective Geometries Over Finite Fields. Oxford Mathematical Monographs. New York: Oxford University Press, 1998.

[15] B. Kim, Y. Lee. The minimum weights of two-point AG codes on norm-trace curves. Finite Fields and their Applications **53**, 113-–139.

[16] S. Lang, A. Weil. Number of points of varieties in finite fields, Amer. J. Math. **76**, 819–827 (1954).

[17] R. Lidl, H. Niederreiter. Finite fields. Vol. 20. Cambridge university press, 1997.

[18] Y.I. Manin, Cubic forms: algebra, geometry, arithmetic. Vol. 4. Elsevier (1986).

[19] C, Marcolla, M. Pellegrini, M. Sala, On the Hermitian curve and its intersection with some conics, Finite Fields and Their Applications 28 (2014) 166–187.

[20] C. Marcolla, M. Pellegrini, M. Sala. On the small-weight codewords of some Hermitian codes. J. Symbolic Comput. **73**, 27–45 (2016).

[21] C. Marcolla, M. Roggero. Minimum-weight codewords of the Hermitian codes are supported on complete intersections, Journal of Pure and Applied Algebra, to appear (https://doi.org/10.1016/j.jpaa.2018.12.007).

[22] G.L. Matthews, *Codes from the Suzuki function field*, IEEE Transactions on Information Theory **50** (12), 3298-3302 (2004).

[23] J.I. Farrán, C. Munuera, G. C. Tizziotti, F. Torres. Gröbner basis for norm-trace codes. Journal of Symbolic Computation **48**, 54–63 (2013).

[24] C. Munuera, G. C. Tizziotti, F. Torres. Two-point codes on Norm-Trace curves. Coding Theory and Applications. Springer, Berlin, Heidelberg. 128–136 (2008).

[25] M. Sala. Gröbner basis techniques to compute weight distributions of shortened cyclic codes. J. Algebra Appl. **6**(3), 403–404 (2007).

[26] H. Stichtenoth. A note on Hermitian codes over $GF(q^2)$. IEEE Trans. Inf. Theory **34**(5), 1345–1348 (1988).

[27] H. Stichtenoth. Algebraic function fields and codes. Graduate Texts in Mathematics **254**, Springer, Berlin (2009).

[28] H.J. Tiersma. Remarks on codes from Hermitian curves. IEEE Trans. Inf. Theory **33**(4), 605–609 (1987).

[29] C.P. Xing, S. Ling. A class of linear codes with good parameters from algebraic curves. IEEE Trans. Inf. Theory **46**(4), 1527–1532 (2000).

[30] K. Yang, P.V. Kumar. On the true minimum distance of Hermitian codes. Coding Theory and Algebraic Geometry **1518**, Lecture Notes in Math., 99–107 (1992).

Matteo Bonini
Department of Mathematics,
University of Trento,
e-mail: matteo.bonini@unitn.it

Massimiliano Sala
Department of Mathematics,
University of Trento,
e-mail: massimiliano.sala@unitn.it