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

Matteo Bonini and Massimiliano Sala

Universitá degli Studi di Trento
matteo.bonini@unitn.it, massimiliano.sala@unitn.it

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, 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 constructed on the curve.

Keywords: Norm-trace curve - AG Code - Weight distribution

1 Introduction

Algebraic-Geometric (AG codes for short) codes form an important class of error correcting codes; see [8, 9, 17].

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: for example the Hermitian curve and its quotients; see for instance [16, 18].

The determination of the intersection of a given curve and low degree curves is often useful for the determination of informations of the algebraic-geometric codes arising from the curve; see [1, 2, 5, 15].

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, 7].

In this paper, we focus our attention on the intersection between the norm-trace curves and the curves of the form $y = ax^3+bx^2+cx+d$ over $\mathbb{F}_{q^3}$, arriving at complete characterization of the intersection between the curve and the parabolas as well as sharp bounds for the other cases. To do so, we employ techniques coming from the properties of irreducible cubic surfaces over finite fields. Then we partially deduce the weight distribution of the corresponding one-point codes.

2 Preliminary Results

Let q be a power of a prime and consider $\mathbb{F}_q$, the finite field with q elements. Let $C \subset (\mathbb{F}_q)^n$ be a linear subspace, then C is a linear code and we will indicate, as usual, with $[n, k, d]$ its parameters, where d is its Hamming minimum distance.

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 $\mathrm{T} = \mathrm{T}_{\mathbb{F}_q}^{\mathbb{F}_{q^r}}$.

This curve $\mathcal{X}$ has $q^{2r-1} + 1$ rational points: q^{2r-1} of them are affine points plus a single point 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 $\left\langle q^{r-1}, \frac{q^r-1}{q-1} \right\rangle$.

Our main aim is the study of the intersection between $\mathcal{X}$ and the cubics of the form $y = ax^3 + bx^2 + cx + d$, where $a, b, c, d \in \mathbb{F}_{q^r}$.

2.2 Algebraic-Geometric Codes

In this section we introduce some basics notions on AG codes. For a detailed introduction we refer to [17].

Let $\mathcal{X}$ be a projective curve over the finite field $\mathbb{F}_q$, consider the rational function field $\mathbb{F}_q(\mathcal{X})$ and the set $\mathcal{X}(\mathbb{F}_q) = \{P_1, \ldots, P_N\}$ given by the $\mathbb{F}_q$-rational places of $\mathcal{X}$. Given an $\mathbb{F}_q$-rational divisor $D = \sum_{i=1,\ldots,n} m_i P_i$, where $n < N$, the Riemann-Roch space associated to D on $\mathcal{X}$ is the vector space $\mathcal{L}(D)$ over $\mathbb{F}_q$ defined as

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

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. We write $\ell(D) = \dim_{\mathbb{F}_q} \mathcal{L}(D)$.

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

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

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 $d \geq d^* = n - \deg(G)$, with 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 space $\mathbb{A}^2(\mathbb{F}_{q^r})$ 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 linear basis $\mathcal{B} = \{w_0, \ldots, w_{r-1}\}$ of $\mathbb{F}_{q^r}$ with respect to $\mathbb{F}_q$, we know that there is a vector space isomorphism $\Phi_{\mathcal{B}} : (\mathbb{F}_q)^r \to \mathbb{F}_{q^r}$ such that $\Phi_{\mathcal{B}}(s_0, \ldots, s_{r-1}) = \sum_{i=0}^{r-1} s_i w_i$. If we consider the maps N,T: $\mathbb{F}_{q^r} \to \mathbb{F}_q$, we can interpret them from $(\mathbb{F}_q)^r$ to $\mathbb{F}_q$ defining $\widetilde{\mathrm{N}} = \mathrm{N} \circ \Phi_{\mathcal{B}}$ and $\widetilde{\mathrm{T}} = \mathrm{T} \circ \Phi_{\mathcal{B}}$. Call $\mathrm{T}_i := \mathrm{T}(A_i x^i)$ 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 $\mathcal{B} = \{\alpha, \alpha^q, \ldots, \alpha^{q^{r-1}}\}$. We know that such a basis exists, see [13, 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

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

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) becomes

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

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 $x_0\alpha + x_1\alpha^q + x_2\alpha^{q^2}$.

Using these relations we can write down equation (3) as follows

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

and we call $\mathcal{S}_1 = \mathcal{S}_1(\overline{\mathbb{F}}_q)$ the surface having this equation, which is clearly defined over $\mathbb{F}_q$.

Remark 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 $y = Ax^2 + Bx + C$.

If we apply the following linear change of coordinates in $\mathrm{GL}(3, \overline{\mathbb{F}}_q)$

$$\begin{cases} X_0 = x_0\alpha + x_1\alpha^q + x_2\alpha^{q^2} \\ X_1 = x_0\alpha^q + x_1\alpha^{q^2} + x_2\alpha \\ X_2 = x_0\alpha^{q^2} + x_1\alpha + x_2\alpha^q \end{cases}$$

we obtain a new surface $\mathcal{S}_2 = \mathcal{S}_2(\overline{\mathbb{F}}_q)$, defined over $\mathbb{F}_{q^3}$, with equation

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

Note that this change of coordinates is bijective since its associated matrix is a Moore matrix, and it is known that its determinant is different from zero since we are dealing with three linearly independent elements, see [13, Corollary 2.38].

Remark 2. Clearly, all the $\mathbb{F}_q$ rational points of $\mathcal{S}_1$ are mapped to all $\mathbb{F}_{q^3}$-rational points of $\mathcal{S}_2$ of the form $(\beta, \beta^q, \beta^{q^2})$, $\beta \in \mathbb{F}_{q^3}$. Similarly, $\mathbb{F}_q$-rational lines contained in $\mathcal{S}_1$ are mapped to $\mathbb{F}_{q^3}$-rational lines contained in $\mathcal{S}_2$ having direction $(\beta, \beta^q, \beta^{q^2})$, $\beta \in \mathbb{F}_{q^3}$. The affinity preserves the absolutely irreducible components of the surfaces and the singularities, since it is in $\mathrm{GL}(3, \overline{\mathbb{F}}_\mathrm{q})$.

Proposition 1. *$\mathcal{S}_1$ is an absolutely irreducible cubic surface.*

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. Using the fact that the surface is irreducible, we can apply the well-known Lang-Weil bound.

Theorem 1 ([12]). *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 1. *The number of $\mathbb{F}_q$-rational points on the surface $\mathcal{S}_1(\mathbb{F}_q)$ is limited by*

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

This bound is better than Bézout's, and other theoretical estimates are known (see [3]), but we want to improve the estimation and arrive at a bound in the form

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

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

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

Conjecture 1. $|\eta| \le 2$ and $\mu = 1$ for all q.

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

Theorem 3 (Theorem 23.1, [14]). *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 $\eta \in \{-2, -1, 0, 1, 2, 3, 4, 5, 7\}$.

Theorem (3) suggests us to to consider separately the case in which $\mathcal{S}_1$ is smooth from the case in which it is singular, indeed (3) gives a good bound for the smooth case.

5 Preliminaries on the singular case

From now on we investigate when $\mathcal{S}_1$ is singular. We start with observing that the possible singular points can only be isolated double points, since $\mathcal{S}_1$ is a cubic irreducible surface. In this context the following result is very helpful.

Theorem 4 ([4]). *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 $\delta \le 4$ 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 [14].

What we want to do now is to find a bound in the desired form for the four possible cases of singularities ($\delta = 1, 2, 3, 4$).

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

$$\begin{cases} X_0X_1X_2 = AX_0^2 + A^qX_1^2 + A^{q^2}X_2^2 + BX_0 + B^qX_1 + B^{q^2}X_2 + D \\ X_1X_2 = 2AX_0 + B \\ X_0X_2 = 2A^qX_1 + B^q \\ X_0X_1 = 2A^{q^2}X_2 + B^{q^2} \end{cases} \tag{6}$$

Remark 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 singular.

Before delving into 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 be special.

Proposition 2. *The possible singular case for $B = 0$ are*

(i) $P = (0, 0, 0)$ *is the only singular point, this happens if and only if $D = 0$.*
(ii) q *is odd and $\delta = 4$, this happens if and only if $-\frac{D}{A}$ is a square. In this case the four singular points cannot be all conjugates with respect to the Frobenius automorphism.*

5.1 One singular point

From now on we can consider $B \neq 0$. From Remark 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

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

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

Proposition 3. *With the same notation as before we have $h = 0$.*

Putting together the previous observations we have the following result.

Proposition 4. *If $\mathcal{S}_1$ has one singular $\mathbb{F}_q$-rational point then*

$$|S_1(\mathbb{F}_q)| \leq q^2 + 1. \tag{7}$$

5.2 Two singular points

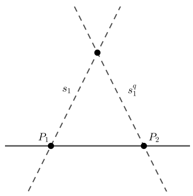
Call P_1 and P_2 the two singular points of $\mathcal{S}_1$, from Remark 3 there are two possibilities:

(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.

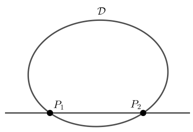
If (i) happens then (7) holds and we can use that bound.

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 [11, 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 [14, Chapter IV]), the first situation can happen at most in 13 cases. Putting together the previous observations we have the following result.

Proposition 5. *If $\mathcal{S}_1$ has two singular $\mathbb{F}_{q^2}$-rational conjugate points then*

$$q^2 - 14q + 39 \leq |S_1(\mathbb{F}_q)| \leq q^2 - q. \tag{8}$$

5.3 Three singular points

Call P_1, P_2 and P_3 the singular points of $\mathcal{S}_1$, from Remark 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 (7) holds, so our task now is to find a bound when (ii) happens.

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 6. *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 $\beta, \gamma \in \mathbb{F}_{q^3}$*

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

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 $z_1 := \frac{1}{r_1}$, $z_2 := \frac{1}{r_2}$ and $z_3 := \frac{1}{r_3}$, 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 $\mathcal{Q}$ is a plane.

Proposition 7. *The quadric surface $\mathcal{Q}$ is absolutely irreducible.*

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. It is widely known (see [10, Section 15.3]) that, in this case

$$|S_1(\mathbb{F}_q)| = q^2 + \eta q + 1, \quad \eta \in \{0, 1, 2\} \tag{9}$$

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

5.4 Four singular points

Call P_1, P_2, P_3 and P_4 the singular points of $\mathcal{S}_1$, applying Remark 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, the last thing we have to do is show that (iii) never holds.

Proposition 8. *Case (iii) never holds.*

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 the ones done for the case $r = 3$ and $h = 2$ we arrive at the situation in which the surface $\widehat{\mathcal{S}}_2$ has equation

$$X_0 X_1 X_2 = A X_0^3 + A^q X_1^3 + A^{q^2} X_2^3 + B X_0^2 + B^q X_1^2 + B^{q^2} X_2^2 + C X_0 + C^q X_1 + C^{q^2} X_2 + E$$

where $E = \mathrm{T}(D)$. The reasonings done above can be completely extended if $\widehat{\mathcal{S}}_1$ is irreducible, so we claim the following result.

Theorem 5. *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 $q^{2r-1} = q^5$ $\mathbb{F}_q$-rational points in $\mathbb{A}^2(\mathbb{F}_q)$. We also know that $\mathcal{L}_{\mathbb{F}_q}(2q^2 P_\infty) = \{ay + bx^2 + cx + d \,|\, a, b, c, d \in \mathbb{F}_{q^3}\}$. Considering the evaluation map

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

the associated one-point code will be $C(D, 2q^2 P_\infty) = \mathrm{ev}(\mathcal{L}_{\mathbb{F}_{q^3}}(2q^2 P_\infty))$, where the divisor D is the formal sum of all the q^5-rational affine points of $\mathcal{X}$. The weight of a codeword associated to the evaluation of a function $f \in \mathcal{L}_{\mathbb{F}_{q^3}}(2q^2 P_\infty)$ 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 $\mathcal{X}$.
   (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 $\mathcal{X}$ 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 6. *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* $\mathrm{w} \geq q^5 - q^2 - 7q - 1$;

Acknowledgements

These results come from the Ph.D thesis of the first author, supervised by the second author.

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. T.D. Browning. *The Lang-Weil estimate for cubic hypersurfaces*, Canad. Math. Bull. **56**, 500–502 (2013).
4. D.F. Coray, M.A. Tsfasman. Arithmetic on singular Del Pezzo surfaces. Proceedings of the London Mathematical Society **3.1**, 25–87 (1988).
5. A. Couvreur, *The dual minimum distance of arbitrary-dimensional algebraic–geometric codes.* Journal of Algebra **350**, 84-107 (2012).
6. 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).
7. O. Geil,(2003). On codes from norm–trace curves. Finite fields and their Applications **9** (3), 351–371.
8. V.D. Goppa. Codes on algebraic curves. Dokl. Akad. NAUK SSSR **259**, 1289–1290 (1981).
9. V.D. Goppa. Algebraic-geometric codes. Izv. Akad. NAUK SSSR **46**, 75–91 (1982).
10. J.W.P. Hirschfeld, Finite projective spaces of three dimensions. Oxford University Press, 1985.
11. J.W.P. Hirschfeld Projective Geometries Over Finite Fields. Oxford Mathematical Monographs. New York: Oxford University Press, 1998.
12. S. Lang, A. Weil. Number of points of varieties in finite fields, Amer. J. Math. **76**, 819–827 (1954).
13. R. Lidl, H. Niederreiter. Finite fields. Vol. 20. Cambridge university press, 1997.
14. Y.I. Manin, Cubic forms: algebra, geometry, arithmetic. Vol. 4. Elsevier (1986).
15. C, Marcolla, M. Pellegrini, M. Sala, On the Hermitian curve and its intersection with some conics, Finite Fields and Their Applications **28**, 166–187 (2014).
16. H. Stichtenoth. A note on Hermitian codes over $GF(q^2)$. IEEE Trans. Inf. Theory **34**(5), 1345–1348 (1988).
17. H. Stichtenoth. Algebraic function fields and codes. Graduate Texts in Mathematics **254**, Springer, Berlin (2009).
18. H.J. Tiersma. Remarks on codes from Hermitian curves. IEEE Trans. Inf. Theory **33**(4), 605–609 (1987).