| Aequationes Mathematicae

Minimal codewords in Norm-Trace codes

Daniele Bartoli, Matteo Bonini, and Marco Timpanella

Abstract. In this paper, we consider the affine variety codes obtained evaluating the polynomials $by = a_k x^k + \ldots + a_1 x + a_0$, $b, a_i \in \mathbb{F}_{q^r}$, at the affine $\mathbb{F}_{q^r}$-rational points of the Norm-Trace curve. In particular, we investigate the weight distribution and the set of minimal codewords. Our approach, which uses tools of algebraic geometry, is based on the study of the absolute irreducibility of certain algebraic varieties.

Mathematics Subject Classification. 14G50, 11T71, 94B27.

Keywords. Norm-trace curve, Minimal codewords, Affine variety codes, Weight spectrum.

1. Introduction

Affine variety codes [1] are linear codes obtained evaluating multivariate polynomials at the $\mathbb{F}_q$-rational points of a certain affine variety. Since any linear code can be described as an affine variety code (see [1, Prop 1.4]), such codes constitute the entire class of linear codes. Even though it is easy to determine the length and the dimension of an affine variety code, a more difficult task is to provide estimates on the minimum distance, or, more generally, on the weight distribution of the code. Still, computing the planar intersections of the chosen variety with some low-degrees ones is often useful in obtaining information on the weight spectrum and the weight distribution of affine-variety codes, see for example [2–6].

Given any linear code C, another challenging task is the determination of the set of its minimal codewords. For a codeword $c \in C$, the *support* of c, denoted by Supp(c), is the set of its nonzero coordinate positions, and the *weight* of c is wt(c) = #Supp(c). If the support of a codeword c contains the support of another codeword c', then we will say that c *covers* c'. A codeword c is said to be *minimal* if it covers only the proportional codewords, i.e. if $c' \in C$ is linearly independent from c, then Supp(c') $\not\subseteq$ Supp(c). Minimal codewords were employed by Massey [7] for the construction of a secret sharing scheme.

For this reason, in recent years, several papers have been dedicated to the determination of the minimal codewords of a linear code [8–17].

In this paper, we give information on the weight distribution and the minimal codewords of affine variety codes arising from the Norm-Trace curve, as already investigated in the literature; see [18–20].In more detail, throughout the paper we consider the affine variety code $C_{q,r,k}$ obtained evaluating the polynomials

$$by = a_k x^k + \ldots + a_1 x + a_0, \tag{1}$$

where $b, a_i \in \mathbb{F}_{q^r}$, at the affine $\mathbb{F}_{q^r}$-rational points of the Norm-Trace curve $\mathcal{N}_{q,r}$, that is the plane curve defined by the affine equation

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

Note that, up to rescaling, we can assume that the polynomials as in (1) are either of type

$$y = a_k x^k + \ldots + a_1 x + a_0, \tag{3}$$

or

$$a_k x^k + \ldots + a_1 x + a_0 = 0.$$

In order to obtain information on the weight distribution of the code $C_{q,r,k}$, we deal with the possible intersection patterns of the curve $\mathcal{N}_{q,r}$ and the curves with affine Equation (3). To do this, our approach is based on the investigation of the absolute irreducibility of a certain algebraic variety, and therefore it relies on tools of algebraic geometry; see Sect. 2 for the details. In the last decades, such tools have proved successful in the construction and investigation of many classes of linear codes; see for instance [5, 21–25].

The paper is organized as follows. The prerequisites on Norm-Trace curves, affine variety codes, and the description of our approach, are give in Sect. 2. Section 3 deals with the absolute irreducibility of an algebraic variety attached to the problem, and these results are then applied in Sect. 4 to investigate the weight distribution of the code $C_{q,r,k}$. Finally, in Sect. 5, we determine the set of minimal codewords of $C_{q,r,k}$.

2. Preliminaries

In this section, we introduce the notation and terminology that we will use throughout the paper. Hereafter, p is a prime and $q = p^m$, where m is a positive integer. Also, $\mathbb{F}_q$ denotes the finite field with q elements. With the symbol $\mathbb{A}^r(\mathbb{F}_q)$ (resp. $\mathbb{P}^r(\mathbb{F}_q)$) we denote the affine (resp. projective) r-dimensional space over $\mathbb{F}_q$.

The norm function $\mathrm{N}_{\mathbb{F}_q}^{\mathbb{F}_{q^r}}$ and the trace function $\mathrm{T}_{\mathbb{F}_q}^{\mathbb{F}_{q^r}}$ are the functions from $\mathbb{F}_{q^r}$ to $\mathbb{F}_q$ defined by

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

and

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

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

2.1. Affine variety codes

We introduce now affine variety codes, see [1] for further information.

Let $t \geq 1$ and consider an ideal $I = \langle g_1, \ldots, g_s \rangle$ of $\mathbb{F}_q[x_1, \ldots, x_t]$, $\{x_1^q - x_1, \ldots, x_t^q - x_t\} \subset I$. The ideal I is zero-dimensional and radical. Let $V(I) = \{P_1, \ldots, P_n\}$ be the variety of I and $R = \mathbb{F}_q[x_1, \ldots, x_t]/I$.

An affine variety code $C(I, L)$ is the image $\phi(L)$ of $L \subseteq R$, an $\mathbb{F}_q$-vector subspace of R of dimension r, given by the isomorphism of $\mathbb{F}_q$-vector spaces $\phi : R \longrightarrow \mathbb{F}_q^n$ that evaluates an element $f \in R$ on $\{P_1, \ldots, P_n\}$, i.e. $\phi(f) = (f(P_1), \ldots, f(P_n))$.

2.2. Norm-trace curve

The Norm-Trace curve $\mathcal{N}_{q,r}$ is the plane curve defined by the affine equation

$$\mathrm{N}_{\mathbb{F}_q}^{\mathbb{F}_{q^r}}(x) = \mathrm{T}_{\mathbb{F}_q}^{\mathbb{F}_{q^r}}(y).$$

The equation $\mathrm{N}_{\mathbb{F}_q}^{\mathbb{F}_{q^r}}(x) = \mathrm{T}_{\mathbb{F}_q}^{\mathbb{F}_{q^r}}(y)$ has precisely q^{2r-1} solutions in $\mathbb{F}_{q^r}^2$, so the curve $\mathcal{N}_{q,r}$ has $q^{2r-1} + 1$ rational points: q^{2r-1} of them correspond to affine points, plus a single point at infinity P_∞. If $r = 2$, $\mathcal{N}_{q,r}$ coincides with the Hermitian curve, whereas $\mathcal{N}_{q,r}$ is singular in P_∞ if $r \geq 3$.

Let $C_{q,r,k}$ be the affine variety code obtained evaluating the polynomials

$$by = a_k x^k + \ldots + a_1 x + a_0,$$

with b and a_i ranging in $\mathbb{F}_{q^r}$, at the q^{2r-1} affine $\mathbb{F}_{q^r}$-rational points of $\mathcal{N}_{q,r}$, and $k < q^{r-1}$. Then $C_{q,r,k}$ has length q^{2r-1}, dimension $k + 1$, and the weight of a codeword associated to the evaluation of a polynomial $by = f(x)$ as in (1) is given by

$$\mathrm{w}(\mathrm{ev}(f)) = q^{2r-1} - |\mathcal{N}_{q,r} \cap \mathcal{X} \cap \mathbb{A}^2(\mathbb{F}_{q^r})|,$$

where $\mathcal{X}$ is the curve with affine equation $by - f(x) = 0$. Therefore, in order to investigate the weight distribution of the code $C_{q,r,k}$, we must study the

possible planar intersections in $\mathbb{A}^2(\mathbb{F}_{q^r})$ between $\mathcal{N}_{q,r}$ and the (rational) curves whose affine equations are given by (1). Here, by planar intersections (or simply intersections) of two curves lying in the affine space $\mathbb{A}^2(\mathbb{F}_{q^r})$, we mean the number of points in $\mathbb{A}^2(\mathbb{F}_{q^r})$ lying on both curves, disregarding multiplicity. Notice that, when b is non-zero then up to rescaling it is possible to assume $b = 1$. For this reason in our investigation we will concentrate on the study of the cases $b = 0$ and $b = 1$.

For the remaining part of this section, we report the approach used in [19,20] to deal with this problem.

In the following we deal with the case $b \neq 0$ in (1). Substituting $y = f(x)$ as in (3) in the equation of $\mathcal{N}_{q,r}$, and exploiting the linearity of the trace function, we get

$$\mathrm{N}(x) = \mathrm{T}(a_k x^k) + \ldots + \mathrm{T}(a_2 x^2) + \mathrm{T}(a_1 x) + \mathrm{T}(a_0). \qquad (4)$$

Now, fix a normal basis $\mathcal{B} = \{\alpha, \alpha^q, \ldots, \alpha^{q^{r-1}}\}$ of $\mathbb{F}_{q^r}$ over $\mathbb{F}_q$ with a suitable $\alpha \in \mathbb{F}_{q^r}$ (see [26] for the details), and let $\Phi_{\mathcal{B}}$ be the canonical vector space isomorphism defined by

$$\Phi_{\mathcal{B}} : (\mathbb{F}_q)^r \longrightarrow \mathbb{F}_{q^r}$$
$$\Phi_{\mathcal{B}}((s_1, \ldots, s_r)) = s_1 \alpha + s_2 \alpha^q + \ldots + s_r \alpha^{q^{r-1}}.$$

This isomorphism allows us to read the norm N and the trace T as maps from $(\mathbb{F}_q)^r$ to $\mathbb{F}_q$, by taking $\widetilde{\mathrm{N}} = \mathrm{N} \circ \Phi_{\mathcal{B}}$ and $\widetilde{\mathrm{T}} = \mathrm{T} \circ \Phi_{\mathcal{B}}$. Let $T_i := T(a_i x^i)$ and $\widetilde{\mathrm{T}}_i := \mathrm{T}_i \circ \Phi_{\mathcal{B}}$, for $1 \leq i \leq k$. Then it is readily seen that $\widetilde{\mathrm{N}}$ and $\widetilde{\mathrm{T}}_i$ are homogeneous polynomials of degrees r and i, respectively, in $\mathbb{F}_q[x_1, \ldots, x_r]$, $i = 0, \ldots, k$.

Therefore, we can rewrite (4) as

$$\widetilde{\mathrm{N}}(x_1, \ldots, x_r) = \widetilde{\mathrm{T}}_k(x_1, \ldots, x_r) + \ldots + \widetilde{\mathrm{T}}_1(x_1, \ldots, x_r) + \mathrm{T}(a_0). \qquad (5)$$

Equation (5) is the equation of a variety $\mathcal{S}$ defined over $\mathbb{F}_q$. Note that the RHS of (5) has degree r, and the LHS has degree k. By construction, the $\mathbb{F}_q$-rational points of $\mathcal{S}$, correspond to the planar intersections in $\mathbb{A}^2(\mathbb{F}_{q^r})$ between the Norm-Trace curve $\mathcal{N}_{q.r}$ and the rational curve of equation $y = f(x)$, see [19, Remark 4.1].

Let $\mathcal{V}_{k,r}$ be the variety $\psi(\mathcal{S})$, where ψ is the affine change of variables of $\mathbb{A}^r(\overline{\mathbb{F}}_q)$ defined by

$$\psi(x_1, \ldots, x_r) = M(x_1, \ldots, x_r)^t = (X_1, \ldots, X_r)^t,$$

and M is the non-singular matrix

$$M = \begin{pmatrix} \alpha & \alpha^q & \ldots & \alpha^{q^{r-1}} \\ \alpha^q & \ldots \alpha^{q^{r-1}} & \alpha \\ \vdots & \vdots & \vdots & \vdots \\ \alpha^{q^{r-1}} & \alpha & \ldots & \alpha^{q^{r-2}} \end{pmatrix}.$$

Then, the variety $\mathcal{V}_{k,r}$ is defined over $\mathbb{F}_{q^r}$, and it has affine equation $V_{k,r}(X_1, \ldots, X_r) = 0$, with

$$V_{k,r}(X_1, \ldots, X_r) = -\prod_{i=1}^{r} X_i + \sum_{i=1}^{r} a_k^{q^{i-1}} X_i^k + \ldots + \sum_{i=1}^{r} a_1^{q^{i-1}} X_i + \mathrm{T}(a_0). \quad (6)$$

Note that ψ is an affine change of variables and thus preserves the number of absolutely irreducible components of $\mathcal{S}$, and their degrees. This equivalence between $\mathcal{V}_{k,r}$ and $\mathcal{S}$ is crucial in our investigation and in the next sections we will make use of this link a number of times.

3. Planar intersections of $\mathcal{N}_{q,r}$ and the curves $y - f(x) = 0$

As it was shown in Sect. 2, finding the planar intersections of the norm-trace curve $\mathcal{N}_{q,r}$ and the curves of Equation (3) is equivalent to finding the number of $\mathbb{F}_q$-rational points of the $\mathbb{F}_q$-rational variety $\mathcal{S}$. Our aim is to prove that $\mathcal{S}$ is absolutely irreducible under certain assumptions on k and r, by proving the absolute irreducibility of $\mathcal{V}_{k,r}$. Indeed, since $\psi(x_1, \ldots, x_r)$ preserves the number of absolutely irreducible components of a variety, it follows that if $\mathcal{V}_{k,r}$ is absolutely irreducible the same holds for $\mathcal{S}$. Also, if $\mathcal{S}$ is absolutely irreducible we can apply the Lang-Weil bound to estimate the number of its $\mathbb{F}_q$-rational points.

Theorem 3.1. *[27, Lang-Weil bound] Let $\mathcal{V} \subset \mathbb{P}^N(\mathbb{F}_q)$ be an absolutely irreducible variety of dimension n and degree d. Then there exists a constant C depending only on N, n, and d such that*

$$\left| \#(\mathcal{V} \cap \mathbb{P}^N(\mathbb{F}_q)) - \sum_{i=0}^{n} q^i \right| \leq (d-1)(d-2)q^{n-1/2} + Cq^{n-1}.$$

Although the constant C was not computed in [27], explicit estimates have been provided for instance in [26, 28–32] and they have the general shape $C = r(d)$ provided that $q > s(n, d)$, where r and s are polynomials of (usually) small degree. We refer to [29] for a survey on these bounds. We only include the following result due to Cafure and Matera.

Theorem 3.2. *[29, Theorem 7.1] Let $\mathcal{V} \subset \mathbb{A}^N(\mathbb{F}_q)$ be an absolutely irreducible variety defined over $\mathbb{F}_q$ of dimension n and degree d. If $q > 2(n+1)d^2$, then the following estimate holds:*

$$|\#(\mathcal{V} \cap \mathbb{A}^N(\mathbb{F}_q)) - q^n| \leq (d-1)(d-2)q^{n-1/2} + 5d^{13/3}q^{n-1}.$$

We report here some results that we will use to prove the irreducibility of $\mathcal{V}_{k,r}$, under certain conditions on k and r. As a corollary of [33, Lemma 4.15], we have the following.

Proposition 3.3. *Let H be a hyperplane of $\mathbb{P}^r(\mathbb{F}_{q^r})$ such that $\mathcal{V}_{k,r} \cap H$ is absolutely irreducibile and of multiplicity one. Then $\mathcal{V}_{k,r}$ is absolutely irreducible.*

The following result about the absolute irreducibility of varieties of Fermat-type is well known and it is a direct consequence of their non-singularity.

Proposition 3.4. *Let n, r be two positive integers such that $p \nmid n$ and $r \geq 3$. Then, the variety of $\mathbb{P}^{r-1}(\overline{\mathbb{F}}_q)$ with homogeneous equation*

$$a_1 X_1^n + a_2 X_2^n + \ldots + a_r X_r^n = 0,$$

where $a_1, \ldots, a_r \in \overline{\mathbb{F}}_q$, is absolutely irreducible.

Proposition 3.5. *Suppose that $k > r \geq 3$ and $p \nmid k$. Then $\mathcal{V}_{k,r}$ is absolutely irreducible.*

Proof. It is readily seen that the homogeneous part in $V_{k,r}$ of the highest degree is

$$\sum_{i=1}^{r} a_k^{q^{i-1}} X_i^k,$$

which is absolutely irreducible by Proposition 3.4. Since $\sum_{i=1}^{r} a_k^{q^{i-1}} X_i^k = 0$ is the intersection between $\mathcal{V}_{k,r}$ and the hyperplane at infinity, it follows that $\mathcal{V}_{k,r}$ is absolutely irreducible by Proposition 3.3. $\square$

Proposition 3.6. *Suppose that $k = r \geq 4$ and $p \nmid k$. Then $\mathcal{V}_{k,r}$ is absolutely irreducible.*

Proof. In this case, the homogeneous part in $V_{k,r}(X_1, X_2, \ldots, X_r)$ of the highest degree is

$$R(X_1, \ldots, X_r) := -\prod_{i=1}^{r} X_i + \sum_{i=1}^{r} a_r^{q^{i-1}} X_i^r.$$

Since $r \geq 4$, the polynomial

$$R(0, X_2, \ldots, X_r) = \sum_{i=2}^{r} a_r^{q^{i-1}} X_i^r$$

is absolutely irreducible by Proposition 3.4, and hence also $R(X_1, \ldots, X_r)$ is absolutely irreducible by Proposition 3.3.

Finally, since $R(X_1, \ldots, X_r) = 0$ is the intersection between $\mathcal{V}_{k,r}$ and the hyperplane at infinity, by Proposition 3.3 the claim follows. $\square$

Proposition 3.7. *Suppose that $k = r \geq 4$ and $p \mid r$. Then $\mathcal{V}_{k,r}$ is absolutely irreducible.*

Proof. Write $r = \bar{r}p^\alpha$, with $p \nmid \bar{r}$. Then $\alpha \geq 1$ and $\bar{r} < r$. The homogeneous part in $V_{k,r}(X_1, X_2, \ldots, X_r)$ of the highest degree is

$$R(X_1, \ldots, X_r) := -\prod_{i=1}^{r} X_i + \sum_{i=1}^{r} a_r^{q^{i-1}} X_i^r = -\prod_{i=1}^{r} X_i + \left(\sum_{i=1}^{r} \bar{a}_r^{q^{i-1}} X_i^{\bar{r}}\right)^{p^\alpha},$$

where $\bar{a}_r^{p^\alpha} = a_r$.

We will prove that $R(X_1, \ldots, X_{r-1}, 1) = 0$ is absolutely irreducible.

Let $F = \sum_{i=1}^{r-1} \bar{a}_r^{q^{i-1}} X_i^{\bar{r}}$. Observe that F is absolutely irreducible by Proposition 3.4. Suppose now that

$$R(X_1, \ldots, X_{r-1}, 1) = G(X_1, X_2, \ldots, X_r)H(X_1, X_2, \ldots, X_r),$$

where $G(X_1, X_2, \ldots, X_r)$ and $H(X_1, X_2, \ldots, X_r)$ have the following shape

$$G(X_1, X_2, \ldots, X_r) = F^\beta + G_{\bar{r}\beta-1} + \ldots + G_0,$$
$$H(X_1, X_2, \ldots, X_r) = F^{p^\alpha - \beta} + H_{(p^\alpha - \beta)\bar{r}-1} + \ldots + H_0,$$

with $0 < \beta < p^\alpha$, and H_i and G_j are either homogeneous polynomials of degree i and j respectively, or they are the zero polynomials. Thus

$$F^\beta H_{(p^\alpha - \beta)\bar{r}-1} + F^{p^\alpha - \beta} G_{\bar{r}\beta-1} = -\prod_{i=1}^{r-1} X_i.$$

This yields $F \mid \prod_{i=1}^{r} X_i$, a contradiction. Therefore $R(X_1, \ldots, X_{r-1}, 1) = 0$ is absolutely irreducible and so is $\mathcal{V}_{r,k}$ by Proposition 3.3. $\qquad\square$

Proposition 3.8. *Suppose that $0 < k < r$. Then $\mathcal{V}_{k,r}$ is absolutely irreducible.*

Proof. If $\mathcal{V}_{k,r}$ is reducible then $V_{k,r}(X_1, X_2, \ldots, X_r)$ splits into the product of two polynomials H and G with the following shape,

$$H(X_1, X_2, \ldots, X_r) = X_1 \ldots X_s + H_{s-1} + \ldots + H_0,$$
$$G(X_1, X_2, \ldots, X_r) = X_{s+1} \ldots X_r + G_{r-s-1} + \ldots + G_0,$$

where H_i and G_j are either homogeneous polynomials of degree i and j respectively, or they are the zero polynomials, and $1 \leq s \leq r - 1$. Let $F_u = \sum_{i=1}^{r} a_u^{q^{i-1}} X_i^u$, then

$$H(X_1, X_2, \ldots, X_r)G(X_1, X_2, \ldots, X_r) = X_1 \cdot \ldots \cdot X_r + \sum_{u=0}^{k} F_u.$$

Because of the shape of $V_{k,r}(X_1, X_2, \ldots, X_r)$, for each i such that $i \geq s+1+k-r$ and $i \leq s-1$, we have that $H_i = 0$. For the same reason, for each j such that $j \geq k-s+1$ and $j \leq r-s-1$, $G_j = 0$.

Now observe that it is not possible that $k - r + s + 1 < 0$ or $k + 1 - s < 0$, otherwise there would exist a variable X_i dividing $H(X_1, X_2, \ldots, X_r)$ or $G(X_1, X_2, \ldots, X_r)$ (and hence dividing $V_{k,r}$).

Therefore, the only possibility left is $k - r + s + 1 \geq 0$ and $k + 1 - s \geq 0$, which gives

$$F_k(X_1, X_2, \ldots, X_r) = X_1 \ldots X_s \cdot G_{k-s}(X_1, X_2, \ldots, X_r) + X_{s+1} \ldots X_r$$
$$\cdot H_{k-r+s}(X_1, X_2, \ldots, X_r).$$

Still, this is not possible, since for $X_1 = 0$ we would have

$$F_k(0, X_2, \ldots, X_r) = \sum_{i=2}^{r} a_k^{q^{i-1}} X_i^k = H_{k-r+s}(0, X_2, \ldots, X_r) \prod_{i=s+1}^{r} X_i.$$

Clearly, this is impossible by Proposition 3.4, as this would imply that $\sum_{i=2}^{r} a_k^{q^{i-1}} X_i^k$ is divisible by $X_{s+1} \cdot \ldots \cdot X_r$. $\qquad\square$

We recall that by the definition of $\mathcal{V}_{k,r}$ and $\mathcal{S}$, these two varieties have the same number of absolutely irreducible components. Therefore, as a byproduct of the previous results, together with Theorem 3.2, we directly obtain the following.

Proposition 3.9. *Let $d = \max(k, r)$, and suppose that one of the following cases holds:*

1. *$k > r$, $p \nmid k$;*
2. *$k = r \geq 4$;*
3. *$0 < k < r$.*

Then, $\mathcal{S}$ is absolutely irreducible and, if $q > 2rd^2$, it contains at least $q^{r-1} - (d-1)(d-2)q^{r-3/2} + 5d^{13/3}q^{r-2}$ points in $\mathbb{A}^r(\mathbb{F}_q)$.

We finally point out that some results for the case $(k, r) = (3, 3)$ and $(k, r) = (3, 2)$ can be found in [20] and [19]), respectively. Unfortunately, it does not seem to be easy to say when $\mathcal{V}_{3,3}$ is irreducible, but when this happens it is possible to give a good estimate on the number of planar intersections between the Norm-Trace curve and rational curves of degree up to three. On the other hand, it is possible to prove (see [19]) that $\mathcal{V}_{2,3}$ is always absolutely irreducible.

4. On the weight spectrum of Norm-Trace codes

Since the codewords of $C_{q,r,k}$ are all given by the evaluations of polynomials of the form $by = f(x)$ as in (1), their weights are then given by

$$\mathrm{w}(\mathrm{ev}(by - f)) = q^{2r-1} - |\mathcal{N}_{q,r} \cap \mathcal{X} \cap \mathbb{A}^2(\mathbb{F}_{q^r})|,$$

where $\mathcal{X}$ is the curve with affine equation $by - f(x) = 0$. Therefore, an estimate on the maximum possible number of $\mathbb{F}_q$-rational planar intersections between $\mathcal{N}_{q,r}$ and the curves $\mathcal{X}$ provides a lower bound on the minimum weight of $C_{q,r,k}$. The case when $b = 0$ was already investigated in [4], while the case

$b \neq 0$ and $\deg(f) \leq 3$ can be found in [19, 20]. Therefore, from now on we will focus on the case $b \neq 0$ and $\deg(f) > 3$.

Classical arguments relying on the Bézout theorem tell us that the number of planar intersections between the two curves can be bounded by the product of the degrees of $\mathcal{N}_{q,r}$ and $\mathcal{X}$. Then, the maximum number of planar intersections is less than or equal to $k\frac{q^r-1}{q-1}$. Therefore the weight of the codewords of $\mathcal{C}_{q,r,k}$ is at least $q^{2r-1} - s\frac{q^r-1}{q-1}$, where $s \leq k$ is the degree of the polynomial whose evaluation defines the codeword.

Still, this result is not tight and, as a byproduct of the results obtained in the previous section, we can give improvements on $\mathrm{d}(C_{q,r,k})$.

Corollary 4.1. *Consider the norm-trace curve $\mathcal{N}_{q,r}$ over the field $\mathbb{F}_{q^r}$, with q large enough, and the code $C = C_{q,r,k}$. Suppose also that one of the following conditions holds*

(a) $k > r$ and $p \nmid k$,
(b) $k = r \geq 4$,
(c) $0 < k < r$.

Let $c = \mathrm{ev}(by - f(x)) \in C$, then:

(i) *If $b = 0$ and f has s distinct roots over $\mathbb{F}_{q^r}$, then $\mathrm{w}(c) = q^{2r-1} - sq^{r-1}$.*
(ii) *If $b \neq 0$ then $\mathrm{w}(c) \geq q^{2r-1} - q^r - 5d^{13/3}q^{r-1} - (k-1)(k-2)q^{\frac{r-1}{2}}$.*

Notice that the case $k = r = 3$ was investigated in [20].

5. Minimal codewords in Norm-Trace codes

First, we investigate the case $k = r = 2$, in which $\mathcal{N}_{q,r}$ coincides with the Hermitian curve $\mathcal{H}$ of homogeneous equation

$$x^{q+1} = y^q + y.$$

In this section we provide a complete classification of the minimal codewords of the affine variety code C obtained by evaluating the polynomials of degree 2 with coefficients in $\mathbb{F}_{q^2}[x, y]$ at the points of $\mathcal{H}$ in $\mathbb{A}^2(\mathbb{F}_{q^2})$, when q is odd. Observe that such a code C contains in particular each codeword of $C_{q,2,2}$. In order to describe the minimal codewords of C, we consider the possible planar intersections in $\mathbb{A}^2(\mathbb{F}_{q^2})$ between $\mathcal{H}$ and the algebraic curves $\mathcal{C}$ described by polynomials of degree 2.

In the case $\mathcal{C}$ is irreducible, i.e. it is an irreducible conic, a complete list of the possible planar intersections between $\mathcal{H}$ and $\mathcal{C}$, which we report below, was given for q odd in [34]. Here, by a subconic of a conic $\mathcal{C}$ we mean $q + 1$ points of $\mathcal{C}$ lying in a Baer subplane $\mathbb{P}^2(\mathbb{F}_q)$ of $\mathbb{P}^2(\mathbb{F}_{q^2})$.

Proposition 5.1. *In $\mathbb{P}^2(\mathbb{F}_{q^2})$, q odd, the intersection pattern of $\mathcal{H}$ and an irreducible conic $\mathcal{C}$ is one of the following.*

   (i) $\mathcal{H} \cap \mathcal{C} = \emptyset$;
  (ii) $|\mathcal{H} \cap \mathcal{C}| = 1$;
 (iii) $|\mathcal{H} \cap \mathcal{C}| = 2$;
 (iv) $|\mathcal{H} \cap \mathcal{C}| = q + 1$. In particular, $\mathcal{H} \cap \mathcal{C}$ is a subconic of $\mathcal{C}$;
  (v) $|\mathcal{H} \cap \mathcal{C}| \in \{2q, 2q + 1, 2q + 2\}$. In particular, $\mathcal{H} \cap \mathcal{C}$ is the union of two
       subconics of $\mathcal{C}$ sharing either zero, one, or two points;
 (vi) $|\mathcal{H} \cap \mathcal{C}| \in \{q, q + 1, q + 2\}$ and meets every subconic of $\mathcal{C}$ in at most four
       points;
(vii) $q - 2\sqrt{q} + 2 \leq |\mathcal{H} \cap \mathcal{C}| \leq q + 2\sqrt{q} + 2$ and meets every subconic of $\mathcal{C}$ in at
       most six points.

   If $\mathcal{C}$ is reducible, the following holds.

Proposition 5.2. In $\mathbb{P}^2(\mathbb{F}_{q^2})$, q odd, the intersection pattern of $\mathcal{H}$ and a re-
ducible conic $\mathcal{C}$ is one of the following.

(viii) If $\mathcal{C}$ is a repeated line ℓ, then either $|\mathcal{H} \cap \mathcal{C}| = 1$ and ℓ is a tangent to $\mathcal{H}$,
       or $|\mathcal{H} \cap \mathcal{C}| = q + 1$ and ℓ is a secant to $\mathcal{H}$;
 (ix) $|\mathcal{H} \cap \mathcal{C}| = 2$ and $\mathcal{C}$ is the product of two distinct tangents to $\mathcal{H}$;
  (x) $|\mathcal{H} \cap \mathcal{C}| \in \{q + 1, q + 2\}$ and $\mathcal{C}$ is the product of a tangent to $\mathcal{H}$ and a
       secant to $\mathcal{H}$;
 (xi) $|\mathcal{H} \cap \mathcal{C}| \in \{2q + 1, 2q + 2\}$ and $\mathcal{C}$ is the product of two distinct secants to
       $\mathcal{H}$.

   We are now in position to prove the main result of this section. Its proof is
based on the observation that a codeword $c \in C$ associated to the evaluation
of a degree 2 polynomial defining a conic $\mathcal{C}$ is minimal if and only if there does
not exist another conic $\mathcal{C}' \neq \mathcal{C}$ such that $\mathcal{H} \cap \mathcal{C} \subseteq \mathcal{H} \cap \mathcal{C}'$.

Proposition 5.3. Let $q > 7$ be odd. With the notations of Propositions 5.1
and 5.2, the minimal codewords of the code C arise from conics whose inter-
section pattern with $\mathcal{H}$ is as in $(iv), (v), (vi), (vii), (xi)$.

Proof. Among the reducible cases, minimal codewords can only arise from
conics that are the product of two distinct secants to $\mathcal{H}$ (case (xi)). Indeed,
the intersection patterns of cases $(viii), (ix), (x)$ are strictly contained in the
intersection of $\mathcal{H}$ with two distinct (properly chosen) secant lines, and hence,
by the above mentioned observation, the corresponding codewords are not
minimal. To prove that a conic $\mathcal{C}$ as in $(iv), (v), (vi), (vii)$ corresponds to a
minimal codeword, assume by way of contradiction that there exists a conic $\mathcal{C}'$
such that $\mathcal{H} \cap \mathcal{C} \subseteq \mathcal{H} \cap \mathcal{C}'$. Then $\mathcal{C} \cap \mathcal{C}'$ contains $\mathcal{H} \cap \mathcal{C}$. However, as $|\mathcal{H} \cap \mathcal{C}| > 4$
holds in each of the cases $(iv), (v), (vi), (vii)$ for $q > 7$, this is in contradiction
to Bézout's Theorem stating that $|\mathcal{C} \cap \mathcal{C}'| \leq 4$. Finally, it is readily seen that
cases $(i), (ii), (iii)$ don't correspond to minimal codewords. $\square$

   From now on in this section we assume $k > 3$, and we give a description of
the minimal codewords of the code $C_{q,r,k}$.

Proposition 5.4. *Let $k < \#\mathcal{N}_{q,r}(\mathbb{F}_{q^r})$. The minimal codewords of $C_{q,r,k}$ are the ones generated by the evaluations of polynomials of the shape*

(i) $y - f(x)$, $\deg(f) = \bar{k}$, *with*

$$q^{r-1} - (\max\{\bar{k}, r\} - 1)(\max\{\bar{k}, r\} - 2)q^{r-3/2} + 5\max\{\bar{k}, r\}^{13/3}q^{r-2} > k,$$

and

$$\bar{k} > r \text{ and } p \nmid \bar{k}, \quad \text{or } \bar{k} = r \geq 4, \quad \text{or } 0 < \bar{k} < r;$$

(ii) $g(x)$, *where $g(x)$ is a polynomial of degree k having all distinct roots in $\mathbb{F}_{q^r}$;*

(iii) $y - \alpha$, *with $\alpha \in \mathbb{F}_{q^r}$.*

Proof. Consider two codewords $c, c' \in C_{q,r,k}$. Recall that the codewords of $C_{q,r,k}$ are the evaluations of polynomials in the span of the set $\{y, x^i\}_{i=0,\ldots,k}$ at the $\mathbb{F}_{q^r}$-rational points of $\mathcal{N}_{q,r}$. Let $F(x,y)$ and $F'(x,y)$ be the polynomials that correspond to c and c', respectively. First, we assume $F(x,y) = f(x)$ and $F'(x,y) = y - g(x)$. Then, we claim that the support of $c = \text{ev}(f(x))$ doesn't contain the support of $c' = \text{ev}(y - g(x))$. Indeed, write $f(x) = \prod_{i=1}^{\deg(f)}(x - t_i)$, with $t_i \in \bar{\mathbb{F}}_q$. Then, the zeros of c correspond to all the affine points of $\mathcal{N}_{q,r}$ with coordinates $(t_i, y_i^{(j)})$ such that $t_i \in \mathbb{F}_{q^r}$ and

$$\text{N}_{\mathbb{F}_q}^{\mathbb{F}_{q^r}}(t_i) = \text{T}_{\mathbb{F}_q}^{\mathbb{F}_{q^r}}(y_i^{(j)}),$$

for $j = 1, \ldots, q^{r-1}$. Observe that if $t_i \notin \mathbb{F}_{q^r}$ for every $i \in \{1, \ldots, \deg(f)\}$, then c is a full-weight codeword and hence it is not minimal. Also, for each $t_i \in \mathbb{F}_{q^r}$, there exists at most a unique $\bar{y}_i$ such that $\bar{y}_i = g(t_i)$ and $(t_i, \bar{y}_i)$ belongs to $\mathcal{N}_{q,r}$. Therefore, the support of c cannot contain the support of c'.

On the other hand, it is readily seen that if $\deg(g) = \bar{k} > 0$, and $\bar{k}$ is as in (i), then the support of c cannot be contained in the support of c'. Indeed, Proposition 3.9 together with the assumption $q^{r-1} - (\max\{\bar{k}, r\} - 1)(\max\{\bar{k}, r\} - 2)q^{r-3/2} + 5\max\{\bar{k}, r\}^{13/3}q^{r-2} > k$, show that the zeros of c cannot contain the zeros of c'.

Now, we deal with the case $F(x,y) = y - f(x)$ and $F'(x,y) = y - g(x)$, with $f(x) \neq g(x)$. Suppose that the zeros of $c = \text{ev}(y - f(x))$ are also zeros of $c' = \text{ev}(y - g(x))$, $f(x) \neq g(x)$. Thus, they are also zeros of $\hat{c} = c - c' = \text{ev}(f(x) - g(x))$. Then, the argument above applied to c and $\hat{c}$ shows that this case is not possible.

Assume now that $F(x,y) = f(x)$ and $F'(x,y) = g(x)$, and denote by $\{t_1, \ldots, t_h\}$ and $\{u_1, \ldots, u_l\}$ the zeros of f and g in $\mathbb{F}_{q^r}$, respectively. Then, it is readily seen that the support of $c = \text{ev}(f(x))$ contains the support of $c' = \text{ev}(g(x))$ if and only if $\{t_1, \ldots, t_h\} \subset \{u_1, \ldots, u_l\}$. As a direct consequence, the minimal codewords arising from a polynomial of type $f(x)$ must be as in Case (ii).

Finally, let $F(x,y) = y - \alpha$ for a certain $\alpha \in \mathbb{F}_{q^r}$. Then, by the above mentioned arguments, together with the fact that the support of c cannot contain the support of a codeword arising from a polynomial of type $y - \beta$, with $\beta \neq \alpha$, we have that in this case c is minimal. $\square$

Acknowledgements

Declarations

Competing interests The authors declare no competing interests.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

References

[1] Fitzgerald, J., Lax, R.F.: Decoding affine variety codes using Gröbner bases. Des. Codes Cryptogr. **13**(2), 147–158 (1998)
[2] Bartoli, D., Bonini, M.: Minimum weight codewords in dual algebraic-geometric codes from the Giulietti-Korchmáros curve. Designs Codes Cryptogr. **87**(6), 1433–1445 (2019)
[3] Couvreur, A.: The dual minimum distance of arbitrary-dimensional algebraic-geometric codes. J. Algebr. **350**(1), 84–107 (2012)
[4] Geil, O.: On codes from norm-trace curves. Finite Fields Appl. **9**(3), 351–371 (2003)
[5] Korchmáros, G., Nagy, G.P., Timpanella, M.: Codes and gap sequences of Hermitian curves. IEEE Trans. Inform. Theory **66**(6), 3547–3554 (2020)

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

[7] Massey, J.L.: Minimal codewords and secret sharing. In Proceedings of the 6th Joint Swedish-Russian International Workshop on Information Theory, pp. 276–279. Citeseer, (1993)

[8] Alfarano, G.N., Borello, M., Neri, A., Ravagnani, A.: Linear cutting blocking sets and minimal codes in the rank metric. J. Comb. Theory Ser. A **192**, 105658 (2022)

[9] Alfarano, G.N., Borello, M., Neri, A., Ravagnani, A.: Three combinatorial perspectives on minimal codes. SIAM J. Discret. Math. **36**(1), 461–489 (2022)

[10] Bartoli, D., Bonini, M., Güneş, B.: An inductive construction of minimal codes. Cryptogr. Commun. **13**(3), 439–449 (2021)

[11] Bartoli, D., Bonini, M., Timpanella, M.: On the weight distribution of some minimal codes. Designs Codes Cryptogr. **89**(3), 471–487 (2021)

[12] Bartoli, D., Martino, B.: Small strong blocking sets by concatenation. SIAM J. Discr. Math. **37**, 6782 (2023)

[13] Bartoli, D., Cossidente, A., Marino, G., Pavese, F.: On cutting blocking sets and their codes. Forum Math. **34**(2), 347–368 (2022)

[14] Bonini, M., Lia, S., Timpanella, M.: Minimal linear codes from hermitian varieties and quadrics. Appl. Algebr. Eng. Commun. Comput. **52**, 1–10 (2021)

[15] Héger, T., Nagy, Z.L.: Short minimal codes and covering codes via strong blocking sets in projective spaces. IEEE Trans. Inform. Theory **68**(2), 881–890 (2021)

[16] Maji, M., Mesnager, S., Sarkar, S., Hansda, K.: On one-dimensional linear minimal codes over finite (commutative) rings. IEEE Trans. Inform. Theory **68**(5), 2990–2998 (2021)

[17] Santonastaso, P., Zullo, F.: On subspace designs. arXiv preprint arXiv:2204.13069, (2022)

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

[19] Bonini, M., Sala, M.: Intersections between the norm-trace curve and some low degree curves. Finite Fields Appl. **67**, 101715 (2020)

[20] Bonini, M., Sala, M., Vicino, L.: Rational points on cubic surfaces and ag codes from the norm-trace curve. Ann. Mat. Pura Appl. **1923**, 1–24 (2022)

[21] Barg, A., Haymaker, K., Howe, E.W., Matthews, G.L., Várilly-Alvarado, A.: Locally recoverable codes from algebraic curves and surfaces. In Algebraic Geometry for Coding Theory and Cryptography. volume 9 of Assoc. Women Math. Ser., pp. 95–127. Springer, Cham (2017)

[22] Lia, S., Timpanella, M.: AG codes from $\mathbb{F}_{q^7}$-rational points of the GK maximal curve. Appl. Algebr. Eng. Commun. Comput. **56**, 1–10 (2021)

[23] Matthews, G.L., Piñero, F.: Codes with locality from cyclic extensions of Deligne-Lusztig curves. Des. Codes Cryptogr. **88**(9), 1909–1924 (2020)

[24] Montanucci, M., Timpanella, M., Zini, G.: AG codes and AG quantum codes from cyclic extensions of the Suzuki and Ree curves. J. Geom. **109**(1), 18–23 (2018)

[25] Timpanella, M., Zini, G.: On a family of linear MRD codes with parameters $[8 \times 8, 16, 7]_q$. Des. Codes Cryptogr. **45**, 1–24 (2023)

[26] Lidl, R., Niederreiter, H.: Finite Fields, vol. 20. Cambridge University Press (1997)

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

[28] Bombieri, E.: Counting points on curves over finite fields. In Séminaire Bourbaki : vol. 1972/73, exposés 418-435, number 15 in Séminaire Bourbaki. Springer-Verlag, (1974). talk:430

[29] Cafure, A., Matera, G.: Improved explicit estimates on the number of solutions of equations over a finite field. Finite Fields Appl. **12**(2), 155–185 (2006)

[30] Ghorpade, S.R., Lachaud, G.: Étale cohomology, Lefschetz theorems and number of points of singular varieties over finite fields. Mosc. Math. J. **2**(3), 589–631 (2002). (**Dedicated to Yuri I. Manin on the occasion of his 65th birthday**)

[31] Ghorpade, S.R., Lachaud, G.: Number of solutions of equations over finite fields and a conjecture of Lang and Weil. In Number Theory and Discrete Mathematics (Chandigarh, 2000), Trends Math., pp. 269–291. Birkhäuser, Basel, (2002)

[32] Schmidt, W.: Equations Over Finite Fields: An Elementary Approach, 2nd edn. Kendrick Press, Heber City (2004)

[33] Bartoli, D.: Hasse-weil type theorems and relevant classes of polynomial functions. London Mathematical Society Lecture Note Series, Proceedings of 28th British Combinatorial Conference, Cambridge University Press (2020)

[34] Donati, G., Durante, N., Korchmáros, G.: On the intersection pattern of a unital and an oval in $\mathrm{PG}(2, q^2)$. Finite Fields Appl. **15**(6), 785–795 (2009)

Daniele Bartoli and Marco Timpanella
Dipartimento di Matematica e Informatica
Università degli Studi di Perugia
Perugia
Italy
e-mail: daniele.bartoli@unipg.it

Marco Timpanella
e-mail: marco.timpanella@unipg.it

Matteo Bonini
Department of Mathematical Sciences
Aalborg University
Aalborg
Denmark
e-mail: mabo@math.aau.dk