Discrete Mathematics 347 (2024) 113835

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

On regular sets of affine type in finite Desarguesian planes and related codes

Angela Aguglia [a,*], Bence Csajbók [a], Luca Giuzzi [b]

[a] Dipartimento di Meccanica, Matematica e Management, Politecnico di Bari, Via Orabona 4, I-70125 Bari, Italy
[b] DICATAM, University of Brescia, Via Branze 53, I-25123 Brescia, Italy

ARTICLE INFO

Article history:
Received 29 May 2023
Received in revised form 18 October 2023
Accepted 30 November 2023
Available online 4 January 2024

Keywords:
Incidence configuration
Projective and affine plane
Unital
Hermitian curve
Linear

ABSTRACT

In this paper, we consider point sets of finite Desarguesian planes whose multisets of intersection numbers with lines are the same for all but one exceptional parallel class of lines. We call such sets *regular of affine type*. When the lines of the exceptional parallel class have the same intersection numbers, then we call these sets *regular of pointed type*. Classical examples are e.g. unitals; a detailed study and constructions of such sets with few intersection numbers is due to Hirschfeld and Szőnyi from 1991. We here provide some general construction methods for regular sets and describe a few infinite families. The members of one of these families have the size as a unital and meet affine lines of $\mathrm{PG}(2,q^2)$ in one of 4 possible intersection numbers, each of them congruent to 1 modulus $\sqrt{q}$.

As a byproduct, we also determine the intersection sizes of the Hermitian curve defined over $\mathrm{GF}(q^2)$, q a square, with suitable rational curves of degree $\sqrt{q}$ and we obtain $\sqrt{q}$-divisible codes with 5 non-zero weights. We also determine the weight enumerator of the codes arising from the general constructions up to some q-powers.

1. Introduction

A classical problem in finite geometry is to construct and characterize sets which have some regularity in their intersection pattern with respect to lines; for example sets with few intersection numbers, sets with a unique intersection number modulus p (the field characteristic), or sets such that for some parallel classes almost all lines of the same class meet the set in the same number of points (possibly modulus p), see [6]. In this paper we consider point sets of finite Desarguesian planes such that the multisets of intersection numbers obtained from different parallel classes of lines are the same for all but one parallel class of lines. We call such sets *regular of affine type*; their formal definition is given in Definition 1.1.

A point set X of $\mathrm{PG}(2,q)$ is of type $(m_1,m_2,\dots,m_k)$ if for each line ℓ of $\mathrm{PG}(2,q)$ there is some $i\in\{1,2,\dots,k\}$ such that $|X\cap\ell|=m_i$. The numbers $m_1,m_2,\dots,m_k$ will be called the *types* of X. It is hard, in general, to find point sets with few types. In [10] Hirschfeld and Szőnyi introduced the notion of *affine type* for those sets of $\mathrm{PG}(2,q)$ which admit at least one tangent line. Assume that P_0 is a point of X and ℓ_0 is a tangent to X at P_0, that is, a line of $\mathrm{PG}(2,q)$ such that $X\cap\ell_0=\{P_0\}$. Up to a suitable choice of reference, we may assume that P_0 is the common point (∞) of all *vertical lines* of affine equation $x=\alpha$ of $\mathrm{AG}(2,q)$ and that $\ell_0=\ell_\infty$ is the line at infinity. Then X is of affine type $(m_1,m_2,\dots,m_k)$ if for each line $\ell\not\ni P_0$ we have $|X\cap\ell|=m_i$ for some $i\in\{1,2,\dots,k\}$. The numbers $m_1,m_2,\dots,m_k$ will be called the *affine*

* Corresponding author.
E-mail addresses: angela.aguglia@poliba.it (A. Aguglia), bence.csajbok@poliba.it (B. Csajbók), luca.giuzzi@unibs.it (L. Giuzzi).

https://doi.org/10.1016/j.disc.2023.113835
0012-365X/

types of X. In [10] the authors proved various results about sets of affine type (m,n) and showed infinite families of such point sets. If in addition all of the vertical lines meet X in the same number of points, say $t+1$ with $t>1$, then X is a *set of pointed type* $[t;m,n]$ (note that these are also sets of type $(1,t+1,m,n)$). The classical examples for such sets are the unitals of $\mathrm{PG}(2,q^2)$; they are exactly the sets of pointed type $[q;1,q+1]$. In [10, Theorem 5.5 for $r=1$ and Theorem 5.8 for $\sqrt{q}\geq r>1$] Hirschfeld and Szőnyi constructed sets of pointed type $[rq;r(q-1),r(q-1)+q]$ in $\mathrm{PG}(2,q^2)$ for q odd. Still for q odd, the same authors constructed also some other sets of pointed type in $\mathrm{PG}(2,q)$ with a small number of affine types. These sets have $s+1$ affine types when s is an even divisor of $q-1$ and $2s+1$ affine types when $s>1$ is an odd divisor of $q-1$, [11, Theorem 3.1]; see after Theorem 2.5 for more details. Another construction appears in [1], where sets of pointed type $[q;q-1,2q-1]$ are constructed in $\mathrm{PG}(2,q^2)$; see Remark 2.8.

As usual, by (d) we denote the common ideal point of the affine lines $y=dx+b$ with slope $d\in\mathrm{GF}(q)$. If X is a set of affine type (m,n) with distinguished point $P_0=(\infty)$ and with tangent $\ell_0=\ell_\infty$ then the number of m-secants and the number of n-secants incident with the direction $(d)\in\ell_\infty$ is the same for each $d\neq\infty$. In this paper we will consider the following generalizations of this concept.

Definition 1.1. A point set X in $\mathrm{PG}(2,q)$ is *regular of affine type* $(m_1,m_2,\dots,m_h)$ if there is a distinguished point P_0 in X and a tangent ℓ_0 of X incident with P_0 such that:

(i) every line not through P_0 is an m_i-secant for some $i\in\{1,2,\dots,h\}$;
(ii) the number of m_i-secants incident with P is the same for each $P\in\ell_0\setminus\{P_0\}$.

The set X is called *regular of pointed type* $[t;m_1,m_2,\dots,m_h]$ for some $t>0$ if in addition to (i) and (ii) it holds that

(iii) all the lines incident with P_0 other than ℓ_0 are $(t+1)$-secants of X.

Finally, a set X in $\mathrm{PG}(2,q)$ is said to be *of pointed type* $[t;m_1,m_2,\dots,m_h]$ if properties (i) and (iii) hold.

Clearly if X is regular of pointed type then it is regular of affine type with the same parameters $(m_1,m_2,\dots,m_h)$. Assuming $P_0=(\infty)$ and $\ell_0=\ell_\infty$, trivial examples of regular sets of affine type are: subsets of a vertical line, the union of some vertical lines, a Baer subplane whose intersection with ℓ_∞ is (∞) and Korchmáros–Mazzocca arcs of type $(0,2,t)$ considered together with their nucleus (here the distinguished point is the nucleus), [14,9]. The point sets constructed in [11, Theorem 3.1] are obtained from a pencil of touching conics. Although it is not mentioned there, sets obtained in this way are necessarily regular of pointed type, see Theorem 2.5. The touching conics idea can be applied to obtain some special examples involving internal and external points of a conic, see Example 2.6.

Let G denote a subgroup of the group of collineations $\mathrm{P\Gamma L}(3,q)$ of $\mathrm{PG}(2,q)$ and denote by $O,O_1,\dots,O_m$ some of the point orbits of G. Put $Y=\cup_{i=1}^k O_i$. Then the multiset $\{|\ell\cap Y|:\ell\ni P\}$ is the same for each choice of $P\in O$. If $O=\ell_\infty$, then Y is an affine set such that the number of k-secants of Y incident with P is the same for each $P\in\ell_\infty$. If $O=\ell_\infty\setminus(\infty)$ then Y is regular of affine type, but not necessarily regular of pointed type, [13].

In Section 2 we consider some general constructions of regular sets of affine type. In particular, in Theorem 2.2 and Theorem 2.3 we show how regular sets of affine type $(m_1,m_2,\dots,m_k)$ in $\mathrm{PG}(2,q)$ may be used to construct regular sets of affine type $(m_1,m_2,\dots,m_k)$ in $\mathrm{PG}(2,q^h)$. This method is a mixture of ideas from [9] and [16].

By Tr and N we will denote the $\mathrm{GF}(q^2)\to\mathrm{GF}(q)$ functions $x\mapsto x+x^q$ and $x\mapsto x^{q+1}$, respectively. For some additive function $f:\mathrm{GF}(q^2)\to\mathrm{GF}(q^2)$ consider the algebraic plane curve of affine equation

$$\mathrm{Tr}(y+f(x))=\mathrm{N}(x). \tag{1}$$

In Theorem 2.7 we show that the set X of the projective points of this curve is regular of pointed type in $\mathrm{PG}(2,q^2)$. Note that this result does not say anything about the affine types, or about the number of affine types. For certain choices of f the resulting point set is a unital and, according to a non-exhaustive computer search for small values of q, when X is not a unital then we have at least 4 affine types (except when q is even and $f(x)=ax^2$, see Remark 2.8 where the non-additive choice $f(x)=ax^2$ is discussed for q odd). Up to equivalence, we found a unique infinite family with 4 affine types, obtained with the choice $f(x)=ax^{\sqrt{q}}$ whenever q is a square prime power and $a\in\mathrm{GF}(q^2)^*$. This case is particular not only because there are few affine types but also because they are all congruent to 1 modulus $\sqrt{q}$ and the point set $X\cup\{(\infty)\}$ meets each line of the plane in 1 modulus $\sqrt{q}$ points. This 1 modulus p property holds only for certain choices of the additive function f.

In Section 3 we determine the affine types of a special point-set of the aforementioned type. This is the most laborious part of our work and it is done separately for the q odd and q even cases. The main result of this section is the following.

Theorem 1.2. *Let q be a square prime power and $a\in\mathrm{GF}(q^2)^*$. Let Γ_a denote the algebraic plane curve of affine equation*

$$\mathrm{Tr}(y+ax^{\sqrt{q}})=\mathrm{N}(x). \tag{2}$$

Then the set of projective points of Γ_a in $\mathrm{PG}(2,q^2)$ is a regular (q^3+1)-set of pointed type

$$[q;\ q-2\sqrt{q}+1,\ q-\sqrt{q}+1, q+1,\ q+\sqrt{q}+1].$$

Using Theorem 1.2, we are able to describe the intersection between an Hermitian curve and a special family of curves of degree $\sqrt{q}$.

Theorem 1.3. *Let q be a square prime power and let $a, m, d \in \mathrm{GF}(q^2)$, $a \neq 0$. Denote by $\mathcal{C}(a, m, d)$ the curve of affine equation $y = ax^{\sqrt{q}} + mx + d$. Then the curves $\mathcal{C}(a, m, d)$ meet the Hermitian curve $y^q + y = x^{q+1}$ of $\mathrm{PG}(2, q^2)$ in the following number of points:*

$$q-2\sqrt{q}+1,\ q-\sqrt{q}+1,\ q+1,\ q+\sqrt{q}+1.$$

We refer the reader to [4] for information about the number of $\mathrm{GF}(q^2)$-rational points in the intersection of a non-degenerate Hermitian surface with a surface of degree-d, where Sørensen's conjecture about the maximal number of such points when $d \le q$ is proven.

In Section 4 we apply Theorem 1.2 to study the projective linear codes associated to Γ_a. These codes are $\sqrt{q}$-divisible with only 5 non-zero weights (when $q = 4$ then with 2 non-zero weights if Γ_a is a unital and with 4 non-zero weights otherwise). We also discuss the corresponding weight enumerators, which are important tools in coding theory, since they contain some crucial information to estimate the actual error-correcting capability and the probability of error-detection and correction of the code with respect to some channels.

2. General constructions of regular sets of affine type

First we show some general results on how to construct new regular sets of affine type starting from a given regular set (of affine type) X. We will always assume that the distinguished point is (∞) and that ℓ_∞ is a tangent to X.

Proposition 2.1.

1. *If X is (regular) of affine type $(m_1, m_2, \dots, m_h)$ in $\mathrm{PG}(2, q)$, then $(\mathrm{AG}(2, q) \setminus X) \cup \{(\infty)\}$ is (regular) of affine type $(q - m_1, q - m_2, \dots, q - m_h)$.*
2. *If X is (regular) of pointed type $[t; m_1, m_2, \dots, m_h]$ in $\mathrm{PG}(2, q)$, then $(\mathrm{AG}(2, q) \setminus X) \cup \{(\infty)\}$ is (regular) of pointed type $[q - t; q - m_1, q - m_2, \dots, q - m_h]$.*

Clearly the same arguments hold in non-Desarguesian finite planes as well. □

The next construction is motivated by [9] and [16]. For $s = h - 1$, this is the same as the construction of [9, Section 3]. When S is a $\mathrm{GF}(p)$-subspace of $\mathrm{GF}(q) \times \mathrm{GF}(q)$, then it is essentially the construction in [16, Section 4]. Our proof here works without assuming the additivity of S.

Theorem 2.2. *Let $S = \{(x_k, y_k)\}_k \subseteq \mathrm{AG}(2, q)$ be a point set such that $S \cup \{(\infty)\}$ is of affine type $(m_1, m_2, \dots, m_g)$. Let $v_1, \dots, v_r$ denote integers such that each vertical line is incident with v_i points of S for some $i \in \{1, 2, \dots, r\}$. Take a non-trivial s-dimensional $\mathrm{GF}(q)$-subspace I of $\mathrm{GF}(q^h)$, with $I \cap \mathrm{GF}(q) = \{0\}$. Consider the point set*

$$S' = \{(x_k, y_k + i) : i \in I,\ (x_k, y_k) \in S\} \subseteq \mathrm{AG}(2, q^h)$$

of size $q^s|S|$. Then the vertical lines of $\mathrm{AG}(2, q^h)$ meet S' in either 0 or in $q^s v_i$ points, for $i \in \{1, 2, \dots, r\}$. Non-vertical lines of $\mathrm{AG}(2, q^h)$ meet S' in either 0, 1 or in m_i points, $i \in \{1, 2, \dots, g\}$. In particular $S' \cup \{(\infty)\}$ is of affine type $(0, 1, m_1, m_2, \dots, m_g)$ and in $\ell_\infty \setminus (\infty)$ there are

(1) q^{s+1} directions (d) incident with $q^h - q^{s+1}$ affine lines that do not meet S' and with $A_{i,d}q^s$ affine lines meeting S' in m_i points. These are exactly the directions (d) with $d \in \mathrm{GF}(q) \oplus I$ and for each such d put $d = d_0 + d_1$ with $d_0 \in \mathrm{GF}(q)$ and $d_1 \in I$. Then for $i \in \{1, 2, \dots, g\}$, $A_{i,d}$ is the number of affine m_i-secants of S in $\mathrm{PG}(2, q)$ incident with the direction $(d_0) \neq (\infty)$ and, $\sum_{i=1}^{g} A_{i,d} = q$;
(2) $q^h - q^{s+1}$ directions incident with $q^s|S|$ tangents to S' and with $q^h - q^s|S|$ affine lines that do not meet S'.

Proof. The statement on the vertical lines is trivial, it remains to determine the size of $S' \cap \ell$, where ℓ is the line of equation $y = dx + b$. This is the same as the cardinality of the set

$$\{(k, i) \in \{1, 2, \dots, |S|\} \times I : y_k + i = dx_k + b\}.$$

Let I' be an $(h - 1)$-dimensional $\mathrm{GF}(q)$-subspace of $\mathrm{GF}(q^h)$ such that $I \subseteq I'$ and $\mathrm{GF}(q) \oplus I' = \mathrm{GF}(q^h)$. For any $e \in \mathrm{GF}(q^h)$ put $e = e_0 + e_1$ with $e_0 \in \mathrm{GF}(q)$ and $e_1 \in I'$.

The condition $y_k + i = dx_k + b$ can be written as $y_k + i = (d_0 + d_1)x_k + b_0 + b_1$, that is,

$$y_k - d_0 x_k - b_0 = d_1 x_k + b_1 - i.$$

Here the left hand side is in GF(q) while the right hand side is in I', thus equality holds if and only if

$$y_k - d_0 x_k - b_0 = 0 \tag{3}$$

and

$$d_1 x_k + b_1 - i = 0. \tag{4}$$

Let ℓ_0 denote the line of equation $y = d_0 x + b_0$ in AG$(2,q)$ and let $w \in \{1, \ldots, g\}$ be such that

$$m_w = |S \cap \ell_0| = |\{(x_k, y_k) : y_k - d_0 x_k - b_0 = 0\}|.$$

(i) If $d_1 \in I$ and $b_1 \in I' \setminus I$ then (4) does not have a solution and hence ℓ meets S' in 0 points.
(ii) If $d_1 \in I$ and $b_1 \in I$ then for every solution (x_k, y_k) of (3) there corresponds a unique solution of (4) and hence ℓ meets S' in m_w points.
(iii) If $d_1 \in I' \setminus I$ then ℓ meets X' in at most one point. Indeed, if we had $d_1 x_k + b_1 = i$ and $d_1 x_{k'} + b_1 = i'$ for some $i, i' \in I$ and $k, k' \in \{1, 2, \ldots, |S|\}$, then $d_1(x_k - x_{k'}) = i - i'$ and hence $d_1 \in I$ would follow, a contradiction.

Since there are $q(q^{h-1} - q^s)$ pairs (d_0, d_1) such that $d_1 \in I' \setminus I$, part *(2)* of the theorem follows from (iii). Since there are $q(q^{h-1} - q^s)$ pairs (b_0, b_1) such that $b_1 \in I' \setminus I$, it follows that each of the q^{s+1} directions (d) such that $d = d_0 + d_1$, $d_1 \in I$ is incident with $q^h - q^{s+1}$ affine lines that do not meet S' (cf. (i)). On the other hand, if $d_1 \in I$ and $b_1 \in I$, then lines with equation $y = dx + b$ meet S' in the same number of points as the line with equation $y = d_0 x + b_0$ meet S (cf. (*ii*)). As there are q^s possible values for b (or choices for b_1) if we fix b_0, this proves part *(1)*. □

Theorem 2.3. *If in Theorem 2.2 the set $S \cup \{(\infty)\}$ is regular of affine type $(m_1, \ldots, m_g)$ in PG$(2,q)$ and $s = h-1$ then $S' \cup \{(\infty)\}$ is regular of affine type $(m_1, \ldots, m_g)$ in PG$(2,q^h)$. Moreover, the number of non-vertical, affine k-secants of S' is a multiple of q^{2h-1} for every integer k.* □

Example 2.4. Theorem 2.2 can also be applied to construct sets with few types. Indeed, if S of PG$(2,q)$ is of type $(0,1,n)$, then S' of PG$(2,q^h)$ is of type $(0,1,n,nq^s)$.

We are going to provide two further constructions of regular sets of pointed type in PG$(2,q)$. The next construction is basically the same as in [10,11]. The difference is that in those papers B is taken as a special subset of GF(q) and the regularity is not explicitly indicated there.

Theorem 2.5. *For $b \in$ GF(q), q odd, let P_b denote the conic of equation $yz = x^2 + bz^2$ in PG$(2,q)$. For $B \subseteq$ GF(q) consider*

$$X(B) := \cup_{b \in B} P_b.$$

Then $X(B)$ is regular of pointed type.

Proof. If $B = \{b_1, b_2, \ldots, b_h\}$ then the vertical lines meet $X(B)$ in $h+1$ points. The line $\ell\colon y = mx + d$ meets $X(B)$ in $2\alpha_{m,d} + \beta_{m,d}$ points where

$$\alpha_{m,d} = |\{b \in B : m^2 - 4(b-d) \text{ is a non-zero square in GF}(q)\}|,$$
$$\beta_{m,d} = |\{b \in B : m^2 - 4(b-d) = 0\}|.$$

Since in the multiset $\{m^2 + 4r : r \in \text{GF}(q)\}$ each element of GF(q) is represented exactly once, it follows that the multiset $\{2\alpha_{m,d} + \beta_{m,d} : d \in \text{GF}(q)\}$ does not depend on the choice of m and hence $X(B)$ is regular of pointed type. □

In [11, Theorem 3.1] it is shown that if $B = \{vu^s : u \in \text{GF}(q)\}$ for some fixed non-square $-v \in$ GF(q) and $s \mid q-1$, s even, then B is of pointed type $[(q-1)/s + 1; 1, m_1, \ldots, m_s]$. Note that with $s = 2$ we obtain the same parameters as in the third subcase of Example!2.6 (cf. the first comment of page 503 of [11] and [3, Section 3.4] from Barlotti, where these sets are considered as complete (k,n)-arcs). On the other hand, if s is an odd divisor of $q-1$, then $X(B)$ is of pointed type $[(q-1)/s + 1; (q-1)/s + 1, m_1, \ldots, m_{2s}]$.

Example 2.6. In PG$(2,q)$ with q odd:

1. the set of the interior points of an oval together with one point of the oval is regular of pointed type $[\frac{1}{2}(q-1); 0, \frac{1}{2}(q-1), \frac{1}{2}(q+1)]$;
2. the set of exterior points of an oval together with one point of the oval is regular of pointed type $[\frac{1}{2}(q-1); q-1, \frac{1}{2}(q-3), \frac{1}{2}(q-1)]$;
3. the set of interior points of an oval united with the set of all the points of the oval is regular of pointed type $[\frac{1}{2}(q+1); 1, \frac{1}{2}(q+3), \frac{1}{2}(q+1)]$;
4. the set of exterior points of an oval united with the set of all the points of the oval is regular of pointed type $[\frac{1}{2}(q+1); q, \frac{1}{2}(q+1), \frac{1}{2}(q-1)]$.

Finally, we consider the pointed sets arising from (1) mentioned in the Introduction.

Theorem 2.7. *If f is an additive $\mathrm{GF}(q^2) \to \mathrm{GF}(q^2)$ function then the set of projective points of the algebraic plane curve X of affine equation*

$$\mathrm{Tr}(y + f(x)) = \mathrm{N}(x)$$

is a regular set of pointed type in $\mathrm{PG}(2, q^2)$. Moreover, in every parallel class of lines the number of k-secants to X is a multiple of q for each integer k.

Proof. It is immediate to see that vertical lines meet X in q affine points. After substituting $y = mx + d$ to determine the number of common points of X and the line $\ell\colon\ y = mx + d$ we obtain

$$m^q x^q + d^q + mx + d + \mathrm{Tr}(f(x)) = x^{q+1}.$$

The number of solutions of this equation remains the same after replacing x by $x + m^q$, thus we obtain:

$$\begin{aligned} m^q(x^q + m) + d^q + m(x + m^q) + d + \mathrm{Tr}(f(x) + f(m^q)) = (x^q + m)(x + m^q) \Leftrightarrow \\ m^q x^q + m^{q+1} + d^q + mx + m^{q+1} + d + \mathrm{Tr}(f(x) + f(m^q)) = x^{q+1} + x^q m^q + mx + m^{q+1} \Leftrightarrow \\ m^{q+1} + \mathrm{Tr}(f(m^q)) + d + d^q = x^{q+1} - \mathrm{Tr}(f(x)). \end{aligned} \tag{5}$$

Denote by $t_{m,d}$ the number of different solutions in x of the equation (5). Recall that $d \mapsto d + d^q$ is q-to-1, hence in the multiset $\{m^{q+1} + \mathrm{Tr}(f(m^q)) + d + d^q : d \in \mathrm{GF}(q^2)\}$ each element of $\mathrm{GF}(q)$ is represented exactly q times. It follows that the multiset $\{t_{m,d} : d \in \mathrm{GF}(q^2)\}$ does not depend on the choice of m and each of its elements is represented a multiple of q times. This completes the proof. □

Remark 2.8. The points of $\mathrm{Tr}(y + f(x)) = \mathrm{N}(x)$ give unitals or regular sets of pointed type $[q; q-1, 2q-1]$ when $f(x) = ax^2$, $a \in \mathrm{GF}(q)^*$, $4\mathrm{N}(a) \neq 1$, q odd. Indeed, in this case the map $x \mapsto x^q - 2ax$ is a bijection of $\mathrm{GF}(q^2)$. The number of solutions of $\mathrm{Tr}(y + ax^2) = \mathrm{N}(x)$, with $y = mx + b$, is the same as the number of solutions of $\mathrm{Tr}(m(x+\alpha) + b + a(x+\alpha)^2) = \mathrm{N}(x+\alpha)$ where α is chosen such that $\alpha^q - 2a\alpha = m$. This equation reads as

$$\mathrm{Tr}(m\alpha + a\alpha^2) - \mathrm{N}(\alpha) + \mathrm{Tr}(b) = \mathrm{N}(x) - \mathrm{Tr}(ax^2).$$

If we view $\mathrm{Tr}(m\alpha + a\alpha^2) - \mathrm{N}(\alpha)$ as a constant and recall that Tr is q-to-1, it is immediate to see that the multiset of the number of solutions in x (as b runs through $\mathrm{GF}(q^2)$) does not depend on the choice of m.

In [1] a very similar construction, related to *Ebert's discriminant condition* ([2,7]), was considered. Applying ideas from there it can be seen that the number of solutions of $\mathrm{Tr}(mx + b + ax^2) = \mathrm{N}(x)$ corresponds to the number of affine points of the conic of equation

$$x_0^2(2a_0 - 1) + x_1^2\varepsilon^2(2a_0 + 1) + 4x_0x_1\varepsilon^2 a_1 + 2x_0m_0 + 2\varepsilon^2 m_1 + 2b_0 = 0$$

of $\mathrm{PG}(2, q)$, where $\varepsilon^{q-1} = -1$ and for each $z \in \mathrm{GF}(q^2)$ we write $z = z_0 + \varepsilon z_1$ with $(z_1, z_2) \in \mathrm{GF}(q)$. When $4\mathrm{N}(a) = 1$ then this conic has a unique point at infinity and hence it has 0, q, or $2q$ affine points, thus we obtain a set of pointed type $[q; 0, q, 2q]$ (which is not regular). On the other hand if $4\mathrm{N}(a) \neq 1$, then to determine the intersection numbers it is enough to consider the case $m = 0$. The conic is reducible if and only if $\mathrm{Tr}(b) = 0$ and it has 1 affine point when $4\mathrm{N}(a) - 1$ is a square and $2q - 1$ affine points when $4\mathrm{N}(a) - 1$ is a non-square in $\mathrm{GF}(q)$. When the curve is irreducible then it has $q + 1$ affine points when $4\mathrm{N}(a) - 1$ is a square and $q - 1$ affine points when $4\mathrm{N}(a) - 1$ is a non-square. Similar ideas work also when q is even and $f(x) = ax^2$. In Section 3 we shall examine the case q square, $f(x) = x^{\sqrt{q}}$.

3. Proofs of Theorems 1.2 and 1.3

3.1. Proof of Theorem 1.2

The odd q case The affinity $\pi: (x, y) \mapsto (\alpha x, y)$ maps the points of the curve $\mathrm{Tr}(y + f(\alpha x)) = \mathrm{N}(\alpha)\mathrm{N}(x)$ to the points of the curve $\mathrm{Tr}(y + f(x)) = \mathrm{N}(x)$. Take some α such that $\mathrm{N}(\alpha) = 2$, with $f(x) = ax^{\sqrt{q}}$. It follows that the set of points of the curve $\mathrm{Tr}(y + a\alpha^{\sqrt{q}}x^{\sqrt{q}}) = 2\mathrm{N}(x)$ is equivalent to Γ_a, which is regular of pointed type by Theorem 2.7. Since $\{a\alpha^{\sqrt{q}} : a \in \mathrm{GF}(q^2)^*\} = \mathrm{GF}(q^2)^*$, to prove Theorem 1.2 it is enough to determine the size of the intersections with lines of $\mathrm{AG}(2, q^2)$ of the curve Λ_a of equation

$$\mathrm{Tr}(y + ax^{\sqrt{q}}) = 2\mathrm{N}(x)$$

with $a \in \mathrm{GF}(q)^*$.

The constant 2 at the right hand side is harmless and just to simplify the computations. Since π fixes (∞), the vertical lines meet Λ_a in the same number of points as they met Γ_a, that is, in q affine points. Since Λ_a is regular of pointed type, it is enough to calculate the size of intersections of Λ_a with horizontal lines. So, after substituting $y = d$, we need to determine the number of solutions of the following equations as d varies in $\mathrm{GF}(q^2)$:

$$a^q x^{\sqrt{q}q} + ax^{\sqrt{q}} + d^q + d - 2x^{q+1} = 0. \tag{6}$$

We can replace x with $xa^{\sqrt{q}}$ in (6) without changing the number of solutions. So we end up with the following

$$\mathrm{N}(a)^{1-\sqrt{q}} x^{\sqrt{q}q} + \mathrm{N}(a)^{1-\sqrt{q}} x^{\sqrt{q}} + d^q/N(a)^{\sqrt{q}} + d/\mathrm{N}(a)^{\sqrt{q}} - 2x^{q+1} = 0.$$

In other words, the number of points of Λ_a in common with the line $y = d$ is the same as the number of points of $\Lambda_{\mathrm{N}(a)^{1-\sqrt{q}}}$ in common with the line $y = d/\mathrm{N}(a)^{\sqrt{q}}$. This means that in (6) we may assume without loss of generality $a \in \mathrm{GF}(q)^*$. For any $a \in \mathrm{GF}(q)^*$, denote by $M_{a,d}$ the number of solutions of (6).

Fix now a primitive element β of $\mathrm{GF}(q^2)$ and put $\varepsilon = \beta^{(q+1)/2}$. Then, $\varepsilon^q = -\varepsilon$ and ε^2 is a primitive element of $\mathrm{GF}(q)$; also $\{1, \varepsilon\}$ is a basis of $\mathrm{GF}(q^2)$ regarded as a vector space over $\mathrm{GF}(q)$. The elements of $\mathrm{GF}(q^2)$ shall always be written as linear combinations with respect to this basis, that is, $z = \hat{z}_0 + \hat{z}_1\varepsilon$, with $z \in \mathrm{GF}(q^2)$ and $\hat{z}_0, \hat{z}_1 \in \mathrm{GF}(q)$. So,

$$\mathrm{Tr}(ax^{\sqrt{q}}) = a(\hat{x}_0^{\sqrt{q}} + \varepsilon^{\sqrt{q}}\hat{x}_1^{\sqrt{q}}) + a(\hat{x}_0^{\sqrt{q}} - \varepsilon^{\sqrt{q}}\hat{x}_1^{\sqrt{q}}) = 2a\hat{x}_0^{\sqrt{q}};$$
$$x^{q+1} = (\hat{x}_0 + \varepsilon\hat{x}_1)(\hat{x}_0 - \varepsilon\hat{x}_1) = (\hat{x}_0^2 - \varepsilon^2\hat{x}_1^2).$$

With this choice of ε, (6) becomes

$$a\hat{x}_0^{\sqrt{q}} - \hat{x}_0^2 + \varepsilon^2\hat{x}_1^2 + \hat{d}_0 = 0, \tag{7}$$

to be solved for $(\hat{x}_0, \hat{x}_1) \in \mathrm{GF}(q)^2$.

Let Ξ be the affine curve of Equation (7) over $\mathrm{GF}(q)$. The number of $\mathrm{GF}(q)$-rational points $P = (\hat{x}_0, \hat{x}_1)$ of Ξ is the number $M_{a,d}$. Rewrite (7) as

$$aX^{\sqrt{q}} - X^2 + \varepsilon^2 Y^2 + t = 0. \tag{8}$$

Let now $\{1, \eta\}$ be a basis of $\mathrm{GF}(q)$ over $\mathrm{GF}(\sqrt{q})$. As before we can choose $\eta \in \mathrm{GF}(q) \setminus \mathrm{GF}(\sqrt{q})$ such that $\eta^{\sqrt{q}} = -\eta$ and η^2 is a primitive element in $\mathrm{GF}(\sqrt{q})$. Set $X = X_0 + \eta X_1$ and $\varepsilon^2 = e$. So,

$$X^2 = (X_0 + \eta X_1)^2 = (X_0^2 + 2\eta X_0X_1 + \eta^2 X_1^2);$$
$$\varepsilon^2 Y^2 = (e_0 + \eta e_1)(Y_0^2 + 2\eta Y_0Y_1 + \eta^2 Y_1^2) = (e_0Y_0^2 + e_0\eta^2Y_1^2 + 2\eta^2 e_1Y_0Y_1) + \eta(e_1Y_0^2 + \eta^2 e_1Y_1^2 + 2e_0Y_0Y_1).$$

Thus, Equation (8) is equivalent to the system of the following two equations

$$t_0 - X_0^2 - \eta^2X_1^2 + e_0Y_0^2 + e_0\eta^2Y_1^2 + 2\eta^2e_1Y_0Y_1 + a_0X_0 - \eta^2a_1X_1 = 0, \tag{9}$$
$$t_1 - 2X_0X_1 + e_1Y_0^2 + \eta^2e_1Y_1^2 + 2e_0Y_0Y_1 + a_1X_0 - a_0X_1 = 0. \tag{10}$$

As both are non-homogeneous quadratic equations in $(X_0, X_1, Y_0, Y_1) \in \mathrm{GF}(\sqrt{q})^4$, the solutions of the system correspond to the affine points of the intersection of two quadratic hypersurfaces $\mathcal{Q}_1$ and $\mathcal{Q}_2$ of $\mathrm{PG}(4, \sqrt{q})$. Thus, the number to determine is $M_{a,d} = |(\mathcal{Q}_1 \cap \mathcal{Q}_2) \setminus \Sigma_\infty|$ where Σ_∞ denotes the hyperplane at infinity. To count the number of these points we first determine the number of points at infinity of $\mathcal{Q}_1 \cap \mathcal{Q}_2$. The matrices associated to the quadrics $\mathcal{Q}_1^\infty = \mathcal{Q}_1 \cap \Sigma_\infty$ and $\mathcal{Q}_2^\infty = \mathcal{Q}_2 \cap \Sigma_\infty$ are respectively

$$A_1^\infty = \begin{pmatrix} -2 & 0 & 0 & 0 \\ 0 & -2\eta^2 & 0 & 0 \\ 0 & 0 & 2e_0 & 2e_1\eta^2 \\ 0 & 0 & 2e_1\eta^2 & 2e_0\eta^2 \end{pmatrix} \tag{11}$$

and

$$A_2^\infty = \begin{pmatrix} 0 & -2 & 0 & 0 \\ -2 & 0 & 0 & 0 \\ 0 & 0 & 2e_1 & 2e_0 \\ 0 & 0 & 2e_0 & 2e_1\eta^2 \end{pmatrix}. \tag{12}$$

We have $\det(A_1^\infty) = 16\eta^4(e_0^2 - \eta^2 e_1^2)$ and $\det(A_2^\infty) = 16(e_0^2 - e_1^2\eta^2)$. Since $\eta \in \mathrm{GF}(q) \setminus \mathrm{GF}(\sqrt{q})$ it follows that $\det(A_1^\infty) \neq 0 \neq \det(A_2^\infty)$ and hence $\mathcal{Q}_1^\infty$ and $\mathcal{Q}_2^\infty$ are always non-singular. Now consider the pencil $\mathcal{F}$ spanned by the two quadrics $\mathcal{Q}_1^\infty$ and $\mathcal{Q}_2^\infty$ over $\mathrm{GF}(q)$. A generic quadric $\mathcal{Q}_{\xi,\lambda}$ with $(\xi,\lambda) \in \mathrm{GF}(\sqrt{q})^2 \setminus \{(0,0)\}$ of $\mathcal{F}$ has matrix

$$A_{\xi,\lambda}^\infty = \begin{pmatrix} -2\xi & -2\lambda & 0 & 0 \\ -2\lambda & -2\eta^2\xi & 0 & 0 \\ 0 & 0 & 2e_0\xi + 2\lambda e_1 & 2\eta^2 e_1\xi + 2\lambda e_0 \\ 0 & 0 & 2\eta^2 e_1\xi + 2\lambda e_0 & 2e_0\eta^2\xi + 2e_1\eta^2\lambda \end{pmatrix} \tag{13}$$

whose determinant is

$$\det(A_{\xi,\lambda}^\infty) = 16(\lambda^2 - \eta^2\xi^2)^2(e_0^2 - e_1^2\eta^2). \tag{14}$$

Observe that $\det(A_{\xi,\lambda}^\infty) = 0$ if and only if either $\eta^2\xi^2 = \lambda^2$ or $\eta^2 = (e_0/e_1)^2$. Since $\eta \notin \mathrm{GF}(\sqrt{q})$ but $\eta^2 \in \mathrm{GF}(\sqrt{q})$, we have that η^2 is a non-square in $\mathrm{GF}(\sqrt{q})$; so, neither of these conditions is possible. Then $\det(A_{\xi,\lambda}^\infty) \neq 0$, $\forall(\xi,\lambda) \in \mathrm{GF}(\sqrt{q})^2 \setminus \{(0,0)\}$. Since $(e_0^2 - \eta^2 e_1^2) = \varepsilon^{2(p+1)}$ is a non-square in $\mathrm{GF}(\sqrt{q})$, all quadrics in $\mathcal{F}$ are elliptic and hence with $q+1$ points. By the argument above, the generic quadric $\mathcal{Q}_{\xi,\lambda}$ of the pencil $\overline{\mathcal{F}}$ spanned by $\mathcal{Q}_1$ and $\mathcal{Q}_2$ has rank at least 4. Let now $\overline{C}$ be the base curve of the pencil $\overline{\mathcal{F}}$. The locus $\overline{C}$ is a quartic curve and the number of its affine rational points over $\mathrm{GF}(\sqrt{q})$ is $M_{a,d}$. If we denote by C the base locus of the pencil $\mathcal{F}$ then we have $|\overline{C}| = M_{a,d} + |C|$.

Observe that

$$|\Sigma_\infty| = |C| + (\sqrt{q}+1)(q+1-|C|),$$

so we get

$$|C| = 0.$$

On the other hand, let r_5, r_4^- be respectively the numbers of non singular quadrics and elliptic cones in $\overline{\mathcal{F}}$. Then,

$$|PG(4,\sqrt{q})| = |\overline{C}| + r_5[(q+1)(\sqrt{q}+1) - |\overline{C}|] + r_4^-[\sqrt{q}(q+1) + 1 - |\overline{C}|],$$

and

$$r_5 + r_4^- = \sqrt{q} + 1.$$

So $|\overline{C}| = r_5\sqrt{q} + 1$ namely $M_{a,d} \equiv 1 \pmod{\sqrt{q}}$. We obtain that $M_{a,d} = (\sqrt{q} + 1 - r_4^-)\sqrt{q} + 1$. We are now going to prove that $r_4^- \leq 3$. To this aim, we compute the number of homogeneous solutions in $\mathrm{GF}(\sqrt{q})^2 \setminus \{(0,0)\}$ of the following equation in (ξ,λ):

$$\det\begin{pmatrix} -2\xi & -2\lambda & 0 & 0 & \xi a_0 + \lambda a_1 \\ -2\lambda & -2\eta^2\xi & 0 & 0 & -(a_1\eta^2\xi + \lambda a_0) \\ 0 & 0 & 2\xi e_0 + 2\lambda e_1 & 2\eta^2 e_1\xi + 2\lambda e_0 & 0 \\ 0 & 0 & 2\eta^2\xi e_1 + 2\lambda e_0 & 2e_0\xi\eta^2 + 2e_1\eta^2\lambda & 0 \\ a_0\xi + \lambda a_1 & -(a_1\eta^2\xi + \lambda a_0) & 0 & 0 & 2(t_0\xi + \lambda t_1) \end{pmatrix} = 0, \tag{15}$$

that is

$$4(e_0^2 - e_1^2\eta^2)(\lambda^2 - \eta^2\xi^2)\det\begin{pmatrix} -2\xi & -2\lambda & \xi a_0 + \lambda a_1 \\ -2\lambda & -2\xi\eta^2 & -(\xi a_1\eta^2 + \lambda a_0) \\ \xi a_0 + \lambda a_1 & -(\xi a_1\eta^2 + \lambda a_0) & 2(\xi t_0 + \lambda t_1) \end{pmatrix} = 0.$$

Since $(\lambda^2 - \eta^2\xi^2)$ is irreducible over $\mathrm{GF}(\sqrt{q})$, the solutions of Equation (15) correspond to those of

$$\det\begin{pmatrix} -2\xi & -2\lambda & \xi a_0+\lambda a_1 \\ -2\lambda & -2\xi\eta^2 & -(\xi a_1\eta^2+\lambda a_0) \\ \xi a_0+\lambda a_1 & -(\xi a_1\eta^2+\lambda a_0) & 2(\xi t_0+\lambda t_1) \end{pmatrix}=0. \tag{16}$$

Suppose now that (16) does not admit solutions of the form $(0,\lambda)$. Then it is possible to divide by ξ, obtaining an equation of degree 3 in λ, which (clearly) has at most 3 different solutions in $\mathrm{GF}(\sqrt{q})$; so $0\le r_4^-\le 3$. On the contrary, if $(0,\lambda)$ is a solution of (16). Then, $-8t_1+4a_0a_1=0$, that is $a_0a_1=2t_1$. Replacing this in (16), we get that the number of homogeneous solutions of (16) is 1 plus the number of isotropic points of the 1-dimensional quadric with matrix

$$\begin{pmatrix} -4t_0+3a_1\eta^2+3a_0 & 4a_0a_1\eta^2 \\ 4a_0a_1\eta^2 & 4\eta^2t_0+a_1\eta^4+a_0\eta^2 \end{pmatrix}.$$

This quadric has at most 2 points, so $1\le r_4^-\le 3$. Consequently, we obtain

$$M_{a,d}\in\{q+1-2\sqrt{q},q+1-\sqrt{q},q+1,q+\sqrt{q}+1\}.$$

The even q case Arguing in the same way as for the q odd case, we see that we have to determine the number of solutions of the following equation

$$\mathrm{N}(a)^{1-\sqrt{q}}x^{\sqrt{q}q}+\mathrm{N}(a)^{1-\sqrt{q}}x^{\sqrt{q}}+d^q/N(a)^{\sqrt{q}}+d/\mathrm{N}(a)^{\sqrt{q}}-x^{q+1}=0, \tag{17}$$

with $a\in\mathrm{GF}(q)^*$ and $d\in\mathrm{GF}(q^2)$.

Fix a primitive element η of $\mathrm{GF}(q^2)\setminus\mathrm{GF}(q)$ such that $\eta^q+\eta=1$ and $\eta^2+\eta+\nu=0$ where $\nu\in\mathrm{GF}(q)\setminus\{1\}$ and $\mathrm{Tr}_{\mathrm{GF}(2)}(\nu)=1$. Then, $\{1,\eta\}$ is a basis of $\mathrm{GF}(q^2)$ regarded as a vector space over $\mathrm{GF}(q)$. The elements of $\mathrm{GF}(q^2)$ shall be written as linear combinations with respect to this basis, that is, $z=\hat{z}_0+\hat{z}_1\eta$, with $z\in\mathrm{GF}(q^2)$ and $\hat{z}_0,\hat{z}_1\in\mathrm{GF}(q)$.

With our choice of η, Equation (17) becomes

$$a\hat{x}_1^{\sqrt{q}}+\hat{d_1}=\hat{x}_0^2+\hat{x}_0\hat{x}_1+\nu\hat{x}_1^2, \tag{18}$$

to be solved for $(\hat{x}_0,\hat{x}_1)\in\mathrm{GF}(q)^2$. Rewrite (18) as

$$aY^{\sqrt{q}}+t=X^2+XY+\nu Y^2, \tag{19}$$

and let $\{1,\gamma\}$ be a basis of $\mathrm{GF}(q)$ over $\mathrm{GF}(\sqrt{q})$. We can choose $\gamma\in\mathrm{GF}(q)\setminus\mathrm{GF}(\sqrt{q})$ such that $\gamma^{\sqrt{q}}+\gamma=1$ and $\gamma^2+\gamma+\nu'=0$ where ν' is an element in $\mathrm{GF}(\sqrt{q})\setminus\{1\}$ whose absolute trace is 1. Setting $X=X_0+\gamma X_1$, $Y=Y_0+\gamma Y_1$ and $\nu=\nu_0+\gamma\nu_1$, (19) is equivalent to the system of the following two equations:

$$X_0^2+\nu'^2X_1^2+\nu_0Y_0^2+\nu'(\nu_0+\nu_1)Y_1^2+X_0Y_0+\nu'X_1Y_1+a_0Y_0+(a_0+\nu'a_1)Y_1+t_0=0, \tag{20}$$

$$X_1^2+[(\nu_0+\nu_1)+\nu'\nu_1]Y_1^2+\nu_1Y_0^2+X_0Y_1+Y_0X_1+X_1Y_1+a_0Y_1+a_1Y_0+t_1=0. \tag{21}$$

As these are non-homogeneous quadratic equations in $(X_0,X_1,Y_0,Y_1)\in\mathrm{GF}(\sqrt{q})^4$, their solutions correspond to the affine points of the intersection of two quadratic hypersurfaces $\mathcal{C}_1$ and $\mathcal{C}_2$ of $\mathrm{PG}(4,\sqrt{q})$.

We refer the reader to [8] for the theory of quadrics in arbitrary (including 2) characteristic. Our approach to study (20) and (21) here is according to [12, Section 1.2]. In particular, we describe the quadrics by means of matrices where we replaced each of the terms a_{ij}'s by formal indeterminates Z_{ij}, then evaluate the discriminant and the Arf invariant as rational functions over the ring of integers $\mathbb{Z}$ and then finally we specialize the indeterminates Z_{ij} to a_{ij} once more. So, the matrices associated to the quadrics $\mathcal{C}_1^\infty:=\mathcal{C}_1\cap\Sigma_\infty$ and $\mathcal{C}_2^\infty:=\mathcal{C}_2\cap\Sigma_\infty$ are

$$P_1^\infty=\begin{pmatrix} 2 & 0 & 1 & 0 \\ 0 & 2\nu' & 0 & \nu' \\ 1 & 0 & 2\nu_0 & 0 \\ 0 & \nu' & 0 & 2\nu'(\nu_0+\nu_1) \end{pmatrix} \tag{22}$$

and

$$P_2^\infty=\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 2 & 1 & 1 \\ 0 & 1 & 2\nu_1 & 0 \\ 1 & 1 & 0 & 2[(\nu_0+\nu_1)+\nu'\nu_1] \end{pmatrix}. \tag{23}$$

We have $\det(P_1^\infty)=\nu'^2\neq 0$ and $\det(P_2^\infty)=1-4\nu_1$, hence $\mathcal{C}_1^\infty$ and $\mathcal{C}_2^\infty$ are both non-singular.

Let

$$B := \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & -1 & 0 & 0 \\ -1 & -1 & 0 & 0 \end{pmatrix}.$$

Since $\dfrac{|B| - 1 + 4\nu_1}{4|B|} = \nu_1$ and

$$\mathrm{Tr}_{\mathrm{GF}(\sqrt{q})|\mathrm{GF}(2)}(\nu_1) = \mathrm{Tr}_{\mathrm{GF}(\sqrt{q})|\mathrm{GF}(2)}(\nu + \nu^{\sqrt{q}}) = \mathrm{Tr}_{\mathrm{GF}(q)|\mathrm{GF}(2)}(\nu) = 1, \tag{24}$$

we have that $\mathcal{C}_2^\infty$ is an elliptic quadric.

Now consider the pencil $\mathcal{F}$ generated by the quadrics $\mathcal{C}_1^\infty$ and $\mathcal{C}_2^\infty$ over GF(q). A generic quadric $\mathcal{C}_{\xi,\lambda} \in \mathcal{F}$ has matrix

$$A_{\xi,\lambda} = \begin{pmatrix} 2\xi & 0 & \xi & \lambda \\ 0 & 2(\lambda + \xi\nu') & \lambda & \lambda + \xi\nu' \\ \xi & \lambda & 2(\xi\nu_0 + \lambda\nu_1) & 0 \\ \lambda & \lambda + \xi\nu' & 0 & 2[(\lambda + \xi\nu')(\nu_0 + \nu_1) + \lambda\nu'\nu_1] \end{pmatrix} \tag{25}$$

whose determinant is

$$\det(A_{\xi,\lambda}) = (\xi^2\nu' + \xi\lambda + \lambda^2)^2. \tag{26}$$

Since $\mathrm{Tr}_{\mathrm{GF}(\sqrt{q})|\mathrm{GF}(2)}\nu' = 1$, we have that $\forall(\xi, \lambda) \in GF(q)^2 \setminus \{(0, 0)\}, \det(A_{\xi,\lambda}) \neq 0$. Thus, each $\mathcal{C}_{\xi,\lambda} \in \mathcal{F}$ is non-singular. For $\xi = 0$ we know that $\mathcal{C}_{0,\lambda}$ is elliptic. We want to prove that $\mathcal{C}_{\xi,\lambda}$ is elliptic also for $\xi \neq 0$. Thus we can assume $\xi = 1$ and set

$$B_\lambda := \begin{pmatrix} 0 & 0 & 1 & \lambda \\ 0 & 0 & \lambda & \lambda + \nu' \\ -1 & -\lambda & 0 & 0 \\ -\lambda & -(\lambda + \nu') & 0 & 0 \end{pmatrix}.$$

We get that

$$\frac{|B_\lambda| - |C_\lambda|}{4|B_\lambda|} = \nu_1$$

and hence, from (24), that $\mathcal{C}_{1,\lambda}$ is an elliptic quadric for all $\lambda \in \mathrm{GF}(\sqrt{q})$. This means that any element of $\mathcal{F}$ is an elliptic quadric. A straightforward computation shows that the determinant of the matrix

$$\overline{A}_{\xi,\lambda} = \begin{pmatrix} 2\xi & 0 & \xi & \lambda & 0 \\ 0 & 2(\lambda + \xi\nu') & \lambda & \lambda + \xi\nu' & 0 \\ \xi & \lambda & 2(\xi\nu_0 + \lambda\nu_1) & 0 & a_0\xi + \lambda a_1 \\ \lambda & \lambda + \xi\nu' & 0 & 2[(\lambda + \xi\nu')(\nu_0 + \nu_1) + \lambda\nu'\nu_1] & a_0(\lambda + \xi) + \xi\nu' a_1 \\ 0 & 0 & \xi a_0 + \lambda a_1 & a_0(\lambda + \xi) + \xi\nu' a_1 & 2(\xi t_0 + \lambda t_1) \end{pmatrix} \tag{27}$$

is the product of $\lambda^2 + \lambda\xi + \nu'\xi^2$, which is an irreducible polynomial over GF($\sqrt{q}$) by a homogeneous polynomial $p(\xi, \lambda)$ of degree 3. If

$$\det(\overline{A}_{\xi,\lambda}) = 0 \tag{28}$$

does not admit solutions of the form $(0, \lambda)$ then we can put $\xi = 1$ in Equation (28) and we end up with an equation of degree 3 in λ which has at most 3 solutions. This implies that there are at most three singular quadrics in the pencil $\overline{\mathcal{F}}$ generated by $\mathcal{C}_1$ and $\mathcal{C}_2$. If $(0, \lambda)$ is a solution of Equation (28) then $\det(\overline{A}_{\xi,\lambda}) = \xi(\xi\lambda^2 + \lambda\xi + \nu'\xi^2)h(\xi, \lambda)$ where $h(\xi, \lambda)$ is a homogeneous polynomial of degree 2. As before if $h(\xi, \lambda)$ is not divisible by ξ, we obtain with a similar argument that $h(1, \lambda)$ has at most 2 roots and we see again that in total there are at most 3 singular quadrics in $\overline{\mathcal{F}}$, one of them being $\mathcal{C}_2$. So we have the following intersection numbers with non-vertical affine lines also for q even:

$$q + 1 - 2\sqrt{q}, q + 1 - \sqrt{q}, q + 1, q + \sqrt{q} + 1.$$

This completes the proof. □

3.2. Proof of Theorem 1.3

The Hermitian curve

$$\mathcal{H}\colon\ y^q + y = x^{q+1} \tag{29}$$

and the curve

$$\mathcal{C}(a,m,d)\colon\ y = ax^{\sqrt{q}} + mx + d,$$

with $a, m, d \in \mathrm{GF}(q^2)$ and $a \neq 0$, share a unique point on the line at infinity, namely the point (∞). On the other hand, the number of affine points lying on both curves is the same as the number of solutions of the system of equations

$$\begin{cases} \mathrm{Tr}(y + ax^{\sqrt{q}}) = \mathrm{N}(x), \\ y = mx + d. \end{cases} \tag{30}$$

This is the same as the number of common points of the line $y = mx + d$ and the curve Γ_a. Then the result follows from Theorem 1.2.

We propose a general conjecture.

Conjecture 1. *Let p be a prime, $h \geq 2$ and $q = p^{2h}$. Then the affine Hermitian curve $\mathcal{H}(q^2)$ of $\mathrm{AG}(2, q^2)$ meets the curves $\mathcal{X}(a,m,d)\colon\ y = ax^p + mx + d$ in 1 modulus p affine points.*

Remark 3.1. As we saw in the proof of Theorem 1.2, the number of lines with slope $m \neq \infty$ and meeting Γ_a in $k_\alpha := (\sqrt{q} + 1 - \alpha)\sqrt{q} + 1$, $\alpha \in \{0, 1, 2, 3\}$ points depends on the parameter a. In fact, for the same q, with different choices of a, we may get point sets with different number of k_α-secants and hence nonequivalent constructions.

The number of k_0, k_1, k_2, k_3-secants of Γ_a with slope $m \neq \infty$ is, respectively is

- either 0, $2^2 \cdot 3$, 0, 2^2, or 2^2, 0, $2^2 \cdot 3$, 0 when $q = 2^2$ (cf. Remark 2.8),
- $3^2 \cdot 2$, $3^2 \cdot 3$, $3^2 \cdot 3$, 3^2 when $q = 3^2$,
- $4^2 \cdot 4$, $4^2 \cdot 6$, $4^2 \cdot 4$, $4^2 \cdot 2$ when $q = 4^2$,
- either $5^2 \cdot 6$, $5^2 \cdot 12$, $5^2 \cdot 3$, $5^2 \cdot 4$, or $5^2 \cdot 7$, $5^2 \cdot 9$, $5^2 \cdot 6$, $5^2 \cdot 3$, when $q = 5^2$.

There are two combinatorially different examples also for $q = 11^2$ and $q = 17^2$.

4. A class of $\sqrt{q}$-divisible codes over GF(q^2) and codes with a simple weight enumerator modulus a q-power

In this section apply the usual construction of codes arising from projective systems to the curve Γ_a. More in detail, we construct a $3 \times (q^3 + 1)$ generator matrix G for a code by taking as columns the coordinates of the points of the algebraic curve Γ_a with Equation (2). The order in which the points are taken is not relevant, as all codes thus obtained are equivalent.

The code $\mathcal{C}(\Gamma_a)$ having G as generator matrix is called *the projective code generated from* Γ_a. The spectrum of the intersections of Γ_a with the lines of $\mathrm{PG}(2, q^2)$ is related to the list of the weights w_i of the associated code; furthermore the minimum Hamming weight of $\mathcal{C}(\Gamma_a)$ is

$$w(\Gamma_a) = |\Gamma_a| - \max\{|\Gamma_a \cap \ell| : \ell \text{ is a line of } \mathrm{PG}(2, q^2)\}.$$

Since $|\Gamma_a| = q^3 + 1$ it is now easy to see that $\mathcal{C}(\Gamma_a)$ is a $[q^3 + 1, 3, q^3 - q - \sqrt{q}]_{q^2}$-linear code. Also, $\mathcal{C}(\Gamma_a)$ has just 5 weights, that is:

$$w_1 = q^3 - q - \sqrt{q},\ w_2 = q^3 - q,\ w_3 = q^3 - q + \sqrt{q},\ w_4 = q^3 - q + 2\sqrt{q},\ w_5 = q^3$$

which are all divisible by $\sqrt{q}$. Furthermore, for $q = 4$, $w_4 = w_5$ and the corresponding $\mathcal{C}(\Gamma_a)$ is either a $[65, 3, 60]_{16}$-linear code with two non-zero weights or a $[65, 3, 58]_{16}$-linear code with just 4 non-zero weights (cf. Remark 3.1).

We define the *intersection enumerator* of the projective curve arising from Γ_a as the polynomial

$$\iota(x) := \sum_{\ell \text{ line of } PG(2,q^2)} x^{|\ell \cap \Gamma_a|} = \sum_i e_i x^i.$$

Denote by A_i the number of codewords of $\mathcal{C}(\Gamma_a)$ with Hamming weight i. The (Hamming) weight enumerator is defined as the polynomial

$$1 + A_1 x + \cdots + A_m x^m;$$

this polynomial gives a great deal of information about the code and is an important invariant. Also, it is used in order to estimate the probability of a successful decoding when there are more than $2d+1$ errors, d being the minimum distance of the code.

If $\iota(x)$ is the intersection enumerator of Γ_a, then the weight enumerator of $\mathcal{C}(\Gamma_a)$ is

$$w(x) = 1 + (q^2-1)\sum e_i x^{q^3+1-i}. \tag{31}$$

From Theorem 1.2, it follows immediately that the only non-zero coefficients in e_i are those for $i \in \{1, q-2\sqrt{q}+1, q-\sqrt{q}+1, q+1, q+\sqrt{q}+1\}$. Also, the only line meeting Γ_a in exactly one point is the line at infinity, and the q^2 vertical lines of $\mathrm{AG}(2,q^2)$ meet Γ_q in $q+1$ points; so $e_1 = 1$. It is easy to see that the following general result holds.

Proposition 4.1. *Let X denote point set of $\mathrm{PG}(2,q^h)$, let $\mathcal{C}(X)$ denote the associated projective code and let e_i denote the coefficient of x^i in $\iota(x)$.*

1. *If X is regular of pointed type then all coefficients e_i with $i \neq 1$ are divisible by q^h, $e_1 \equiv 1 \pmod{q^h}$.*
2. *If $h=2$ and X is obtained from Theorem 2.7 (such as Γ_a) then all coefficients e_i with $i \notin \{1, q+1\}$ are divisible by q^3, $e_{q+1} \equiv q^2 \pmod{q^3}$ and $e_1 \equiv 1 \pmod{q^3}$.*
3. *If $X = S' \cup \{(\infty)\}$ is obtained from a regular set S of pointed type $[t; m_1, \ldots, m_g]$ of $\mathrm{PG}(2,q)$ as in Theorem 2.2, then all coefficients e_i with $i \notin \{1, q^st+1\}$ are divisible by q^{2s+1}, $e_{q^st+1} = q$, $e_1 \equiv q^h - q + 1 \pmod{q^{2s+1}}$.* □

The result above has the following immediate consequence.

Proposition 4.2. *If X is regular of pointed type in $\mathrm{PG}(2,q^h)$, $\mathcal{C}(X)$ denote the associated projective code and e_i denote the coefficient of x^i in $\iota(x)$, then the weight enumerator $1+(q^h-1)\sum e_i x^{|X|-i}$ of $\mathcal{C}(X)$ modulus q^h equals*

$$1 - x^{|X|-1}.$$

If $h=2$ and X is obtained from Theorem 2.7 (such as Γ_a) then the weight enumerator of $\mathcal{C}(x)$ modulus q^3 equals

$$1 - q^2 x^{q^3-q} + (q^2-1)x^{q^3}.$$

If $X = S' \cup \{(\infty)\}$ is obtained from a regular set S of pointed type $[t; m_1, \ldots, m_g]$ of $\mathrm{PG}(2,q)$ as in Theorem 2.2, then the weight enumerator of $\mathcal{C}(x)$ modulus q^{2s+1} equals

$$1 + (q^{h+1}-q)x^{tq^s(q-1)} + (-q^{h+1}+q-1)x^{tq^{s+1}}. \quad \square$$

Observe that the codes $\mathcal{C}(\Gamma_a)$ not only have good parameters, but they turn also out to be $\sqrt{q}$-divisible, see [15,17]. Incidentally, as the codes we consider are projective, their duals are $[q^3+1, q^3-3, 3]$-linear almost MDS codes (however they are not NMDS), see [5].

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Acknowledgement

This work was supported by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA–INdAM) and partially supported by the European Union under the Italian National Recovery and Resilience Plan (NRRP) of NextGenerationEU, partnership on “Telecommunications of the Future” (PE00000001 - program “RESTART”, CUP: D93C22000910001). The second author acknowledges the partial support of the National Research, Development and Innovation Office – NKFIH, grant no. K 124950.

References

[1] A. Aguglia, G. Korchmáros, Multiple blocking sets and multisets in Desarguesian planes, Des. Codes Cryptogr. 56 (2010) 177–181.
[2] R.D. Baker, G.L. Ebert, On Buekenhout–Metz unitals of odd order, J. Comb. Theory, Ser. A 60 (1) (1992) 67–84.
[3] A. Barlotti, Some topics in finite geometrical structures, Institute of Statistics, University of North Carolina, 1965, mimeo series No. 439.
[4] P. Beelen, M. Datta, M. Homma, A proof of Sørensen's conjecture on Hermitian surfaces, Proc. Am. Math. Soc. 149 (2021) 1431–1441.
[5] M.A. De Boer, Almost MDS codes, Des. Codes Cryptogr. 9 (2) (1996) 143–155.
[6] B. Csajbók, P. Sziklai, Zs. Weiner, Renitent lines, Eur. J. Comb. 114 (2023).
[7] G.L. Ebert, On Buekenhout–Metz unitals of even order, Eur. J. Comb. 13 (2) (1992) 109–117.
[8] R. Elman, N. Karpenko, A. Merkurjev, The Algebraic and Geometric Theory of Quadratic Forms, AMS Colloquium Publications, vol. 56, AMS, 2008.
[9] A. Gács, Zs. Weiner, On $(q+t,t)$-arcs of type $(0,2,t)$, Des. Codes Cryptogr. 29 (2003) 131–139.
[10] J.W.P. Hirschfeld, T. Szőnyi, Sets in a finite plane with few intersection numbers and a distinguished point, Discrete Math. 97 (1991) 229–242.
[11] J.W.P. Hirschfeld, T. Szőnyi, Constructions of large arcs and blocking sets in finite planes, Eur. J. Comb. (1991) 499–511.
[12] J.W.P. Hirschfeld, J.A. Thas, General Galois Geometries, Springer-Verlang, London, 2016.
[13] G. Korchmáros, Private communication, 2023.
[14] G. Korchmáros, F. Mazzocca, On $(q+t)$-arcs of type $(0,2,t)$ in a Desarguesian plane of order q, Math. Proc. Camb. Philos. Soc. 108 (1990) 445–459.
[15] S. Kurz, Divisible codes, https://arxiv.org/abs/2112.11763.
[16] V. Napolitano, O. Polverino, P. Santonastaso, F. Zullo, Classifications and constructions of minimum size linear sets, Finite Fields Appl. 92 (2023).
[17] H.N. Ward, Divisible codes – a survey, Serdica Math. J. 27 (2001) 263–278.