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

Angela Aguglia

(Joint work with Bence Csajbók and Luca Giuzzi)

Dipartimento di Meccanica, Matematica e Management
Politecnico di Bari

CODESCO'24
9^{th} July, Sevilla

- A point set X of $\mathrm{PG}(2, q)$ is *of type* $(m_1, m_2, \ldots, m_k)$ if for each line ℓ of $\mathrm{PG}(2, q)$ there is some $i \in \{1, 2, \ldots, k\}$ such that $|X \cap \ell| = m_i$.

- The numbers $m_1, m_2, \ldots, m_k$ are called the *types* of X.

- It is hard, in general, to find point sets with few types.

- Hirschfeld and Szőnyi in 1991 introduced the notion of *affine type* for those sets of $\mathrm{PG}(2, q)$ which admit at least one tangent line.

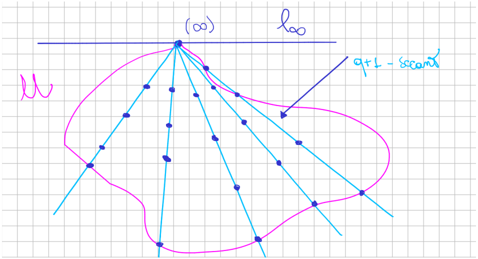
- Assume that P_0 is a point of X and ℓ_0 is a tangent to X at P_0, that is, $X \cap \ell_0 = \{P_0\}$.
- We may assume that P_0 is the common point (∞) of all *vertical lines* of affine equation $x = \alpha$ of $\mathrm{AG}(2, q)$ and that $\ell_0 = \ell_\infty$ is the line at infinity.
- Then X is *of affine type* $(m_1, m_2, \ldots, m_k)$ if for each line $\ell \not\ni P_0$ we have $|X \cap \ell| = m_i$ for some $i \in \{1, 2, \ldots, k\}$.
- The numbers $m_1, m_2, \ldots, m_k$ are called the *affine types* of X.

- 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 $d \neq \infty$.

- If in addition all of the vertical lines meet X in the same number of points, say $t+1$ with $t>0$, then X is a *set of pointed type* $[t; m, n]$.

- The classical examples for such sets are the unitals of $\mathrm{PG}(2, q^2)$; they are exactly the sets of pointed type $[q; 1, q+1]$.



The generalization of these concepts is the following.

Definition 1

A point set X in $\mathrm{PG}(2,q)$ is *regular of affine type* $(m_1, m_2, \ldots, m_h)$ 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 $i \in \{1, 2, \ldots, h\}$;

(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* $[t; m_1, m_2, \ldots, m_h]$ for some $t > 0$ if in addition to (i) and (ii) it holds that

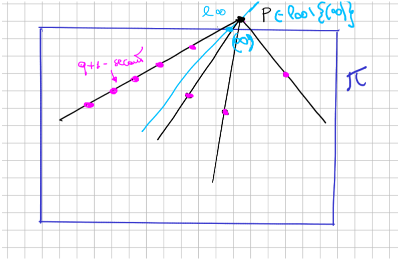
(iii) all the lines incident with P_0 other than ℓ_0 are $(t+1)$-secants of X.

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

If X is regular of pointed type then it is regular of affine type with the same parameters $(m_1, m_2, \ldots, m_h)$.

Assuming $P_0 = (\infty)$ and $\ell_0 = \ell_\infty$, examples of regular sets of affine type are:

- subsets of a vertical line;
- the union of some vertical lines;
- a Baer subplane π whose intersection with ℓ_∞ is (∞).



Examples of regular sets of pointed type:

the point sets constructed by Hirschfeld and Szőnyi in:

- J.W.P. Hirschfeld, T. Szőnyi: *Constructions of large arcs and blocking sets in finite planes*, Eur. J. Comb. (1991), 109–117.

which are obtained from a pencil of touching conics.

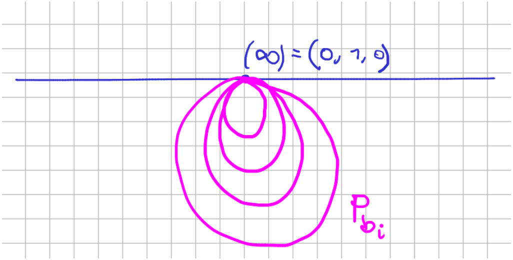
Our constructions of regular sets of pointed type.

Theorem 2 (A. A., B. Csajbók, L. Giuzzi (2024))

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

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

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



- 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.

Theorem 3 (A. A., B. Csajbók, L. Giuzzi (2024))

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.

- 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 $f(x) = ax^2$).

- 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.

Theorem 4 (A. A., B. Csajbók, L. Giuzzi (2024))

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

$$\mathrm{Tr}\,(y + ax^{\sqrt{q}}) = \mathrm{N}(x). \tag{1}$$

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

Theorem 5 (A. A., B. Csajbók, L. Giuzzi (2024))

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 propose a general conjecture.

Conjecture 1

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

- 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.

- The number of k_0, k_1, k_2, k_3-secants of Γ_a with slope $m \neq \infty$ respectively is
  - either 0, $2^2 \cdot 3$, 0 , 2^2, or 2^2, 0, $2^2 \cdot 3$, 0 when $q = 2^2$,
  - $3^2 \cdot 2$, $3^2 \cdot 3$, $3^2 \cdot 3$, 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 $q = 17^2$.

- We apply Theorem 4 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 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 (1).
- 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.

- 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

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

- The weight enumerator gives a great deal of information about the code. 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
- $$w(x) = 1 + (q^2 - 1) \sum e_i x^{q^3+1-i}. \qquad (2)$$
- The only non-zero coefficients 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_a in $q + 1$ points; so $e_1 = 1$.

- Observe that the codes $\mathcal{C}(\Gamma_a)$ not only have good parameters, but they turn also out to be $\sqrt{q}$-divisible.

- Incidentally, as the codes we consider are projective, their duals are $[q^3+1, q^3-2, 3]$-linear almost MDS codes (however, they are not NMDS).

Open Problem

- Find some new additive functions $f : \mathrm{GF}(q^2) \to \mathrm{GF}(q^2)$ such that the set of projective points of the algebraic plane curve X of affine equation

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

which is regular of pointed type, has very few types.

- This work was 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).

Thank you

for your attention!