Intersection problem for linear sets in the projective line

Ferdinando Zullo

8th Polish Combinatorial Conference

September 14-18, 2020
eConference

Università degli Studi della Campania *Luigi Vanvitelli*

Dipartimento di Matematica e Fisica

G. Zini and FZ
"On the intersection problem for linear sets in the projective line"
arXiv:2004.09441 [Math.CO]

Università
degli Studi
della Campania
Luigi Vanvitelli

Introduction

The problem of determining how can intersect each other two geometric/algebraic/combinatorial objects in a fixed family is well-studied

- Finite Geometries;
- Coding Theory;
- Graph Theory;
- Computational Geometry;
- Cryptography;
- etc…

The problem of determining how can intersect each other two geometric/algebraic/combinatorial objects in a fixed family is well-studied

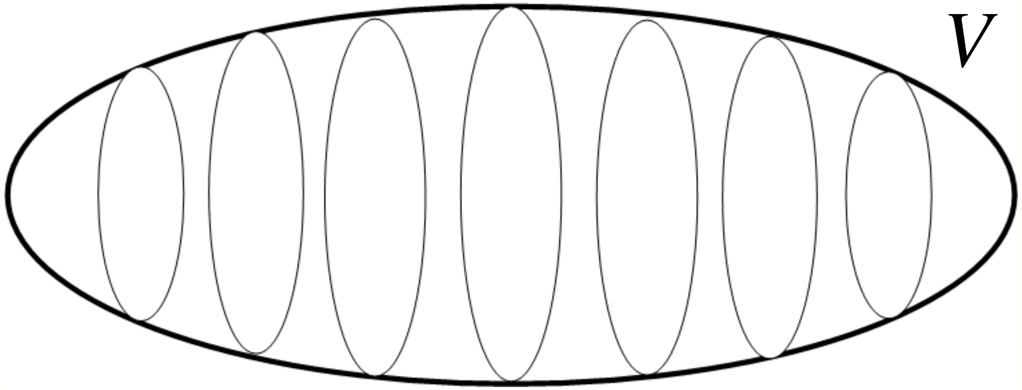
- Finite Geometries;
- Coding Theory;
- Graph Theory;
- Computational Geometry;
- Cryptography;
- etc…

We will analyze the intersection problem for linear sets

Linear sets

Linear sets

$$V = V(r, q^n) = V(rn, q)$$

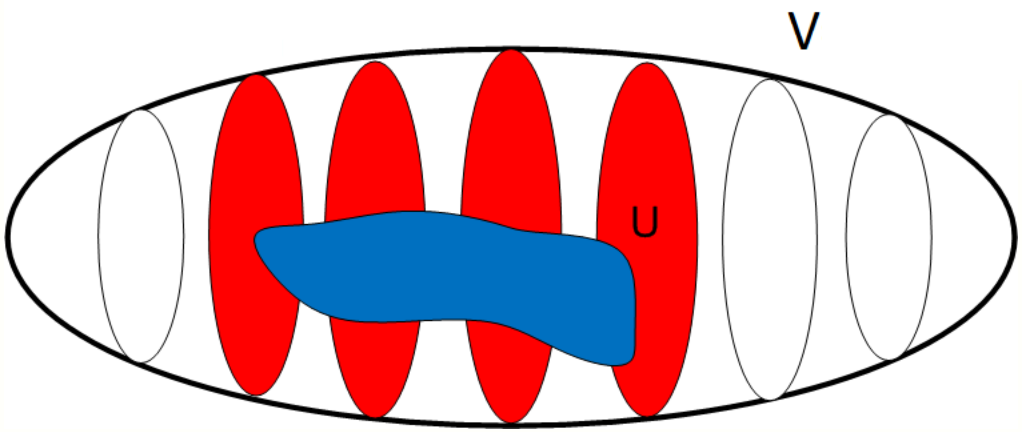


$S = \{\langle \mathbf{u} \rangle_{\mathbb{F}_{q^n}} : \mathbf{u} \in V \setminus \{\mathbf{0}\}\}$ Desarguesian spread of V

$S \mapsto$ points of $\mathrm{PG}(r-1, q^n)$

Linear sets

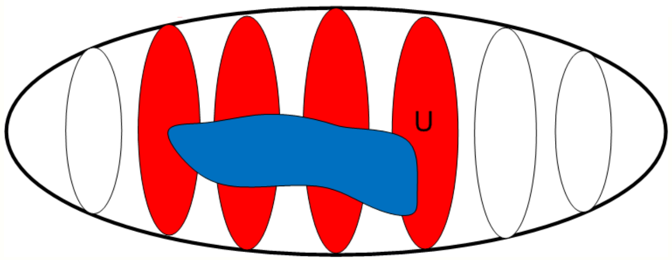
Let U be an $\mathbb{F}_q$-subspace of $V = V(r, q^n)$



$$S = \{\langle \mathbf{u} \rangle_{\mathbb{F}_{q^n}} : \mathbf{u} \in V \setminus \{\mathbf{0}\}\}$$

Linear sets

Let U be an $\mathbb{F}_q$-subspace of $V = V(r, q^n)$



$$L_U = \{\langle \mathbf{u} \rangle_{\mathbb{F}_{q^n}} : \mathbf{u} \in U \setminus \{\mathbf{0}\}\}$$

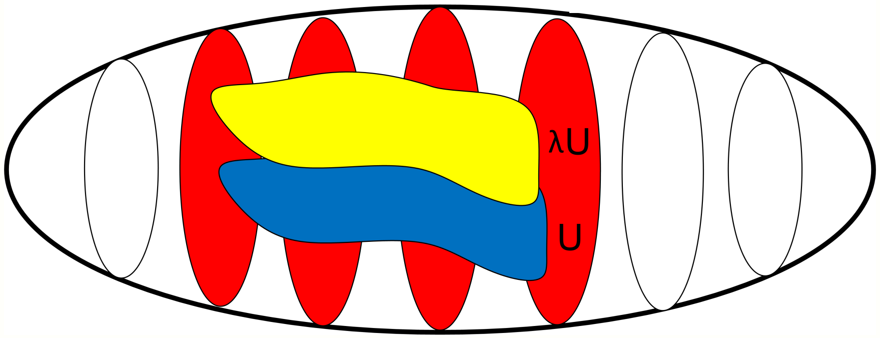
L_U is said $\mathbb{F}_q$-linear set of $\mathrm{PG}(V, \mathbb{F}_{q^n}) = \mathrm{PG}(r-1, q^n)$

Rank of L_U is $\dim_{\mathbb{F}_q} U$

G. Lunardon
"Normal spreads"
Geom. Dedicata **75** (1999) 245-261.

Linear sets

Let U be an $\mathbb{F}_q$-subspace of $V = V(r, q^n)$



$$L_U = \{\langle \mathbf{u} \rangle_{\mathbb{F}_{q^n}} : \mathbf{u} \in U \setminus \{\mathbf{0}\}\}$$

L_U is said $\mathbb{F}_q$-linear set of

$\mathrm{PG}(V, \mathbb{F}_{q^n}) = \mathrm{PG}(r-1, q^n)$

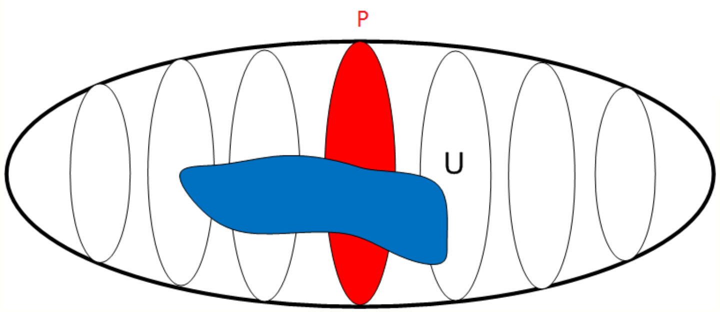
Let $\lambda \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$, then

$\lambda U \neq U$ and $L_U = L_{\lambda U}$

Università
degli Studi
della Campania
Luigi Vanvitelli

Linear sets

Let U be an $\mathbb{F}_q$-subspace of $V = V(r, q^n)$



$$L_U = \{\langle \mathbf{u} \rangle_{\mathbb{F}_{q^n}} : \mathbf{u} \in U \setminus \{\mathbf{0}\}\}$$

$$P = \langle \mathbf{v} \rangle_{\mathbb{F}_{q^n}} \in \mathrm{PG}(r-1, q^n)$$

$$w_{L_U}(P) = \dim_{\mathbb{F}_q}(U \cap \langle \mathbf{v} \rangle_{\mathbb{F}_{q^n}})$$

Weight of P in L_U

Examples of linear sets: projective subspaces

Let U be an $\mathbb{F}_{q^n}$-subspace of $V = V(r, q^n)$ of dimension h

$$L_U = \{\langle \mathbf{u} \rangle_{\mathbb{F}_{q^n}} : \mathbf{u} \in U \setminus \{\mathbf{0}\}\} = \mathrm{PG}(h-1, q^n)$$

$\mathbb{F}_q$-linear set of rank hn

$\mathbb{F}_{q^n}$-linear set of rank h

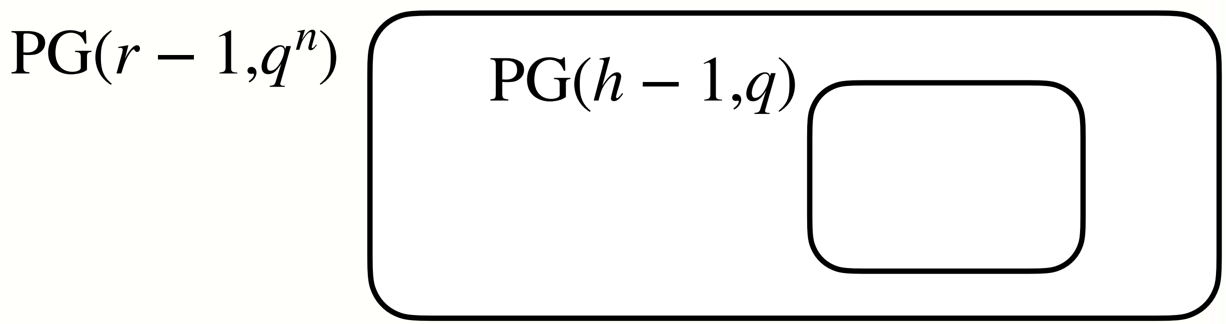
Examples of linear sets: subgeometries

Let U be an $\mathbb{F}_q$-subspace of $V = V(r, q^n)$ of dimension h s.t.

$\dim_{\mathbb{F}_{q^n}} \langle U \rangle_{\mathbb{F}_{q^n}} = h$ then

$$L_U = \{\langle \mathbf{u} \rangle_{\mathbb{F}_{q^n}} : \mathbf{u} \in U \setminus \{\mathbf{0}\}\} = \mathrm{PG}(h-1, q) \subseteq \mathrm{PG}(r-1, q^n)$$

$\mathbb{F}_q$-linear set of rank h



Examples of linear sets: subgeometries

Let U be an $\mathbb{F}_q$-subspace of $V = V(r, q^n)$ of dimension h s.t.

$\dim_{\mathbb{F}_{q^n}} \langle U \rangle_{\mathbb{F}_{q^n}} = h$ then

$$L_U = \{\langle \mathbf{u} \rangle_{\mathbb{F}_{q^n}} : \mathbf{u} \in U \setminus \{\mathbf{0}\}\} = \mathrm{PG}(h-1, q) \subseteq \mathrm{PG}(r-1, q^n)$$

$\mathbb{F}_q$-linear set of rank h

Example:

Let $V = \mathbb{F}_{q^n}^r$ and $U = \mathbb{F}_q^r$, then L_U is an $\mathbb{F}_q$-linear set of rank r.

Examples of linear sets: subgeometries

Let $V = \mathbb{F}_{q^n}^n$ and let

$$U = \{(x, x^q, \ldots, x^{q^{n-1}}) : x \in \mathbb{F}_{q^n}\}$$

$$L_U = \{\langle \mathbf{u} \rangle_{\mathbb{F}_{q^n}} : \mathbf{u} \in U \setminus \{\mathbf{0}\}\} = \mathrm{PG}(n-1, q) \subseteq \mathrm{PG}(n-1, q^n)$$

$\mathbb{F}_q$-linear set of rank n

Intersection problem for linear sets

Problem

Consider any two $\mathbb{F}_q$-linear sets L_{U_1} and L_{U_2} of $\mathrm{PG}(r-1, q^n)$ then

$$L_{U_1} \cap L_{U_2}?$$

Hard Problem in general!

Let L_{U_1} and L_{U_2} two $\mathbb{F}_q$-linear sets then

$$L_{U_1} \cap L_{U_2} \supseteq L_{U_1 \cap U_2}$$

But in general $L_{U_1} \cap L_{U_2} \neq L_{U_1 \cap U_2}$!

Example

Let L_U be an $\mathbb{F}_q$-linear set in $\mathrm{PG}(r-1, q^n)$ and let $\lambda \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$, then

$$L_U \cap L_{\lambda U} = L_U \text{ but } L_{U \cap \lambda U} = \emptyset$$

Let $\Omega = \mathrm{PG}(W, \mathbb{F}_{q^n})$ be a subspace of $\mathrm{PG}(r-1, q^n)$

Let L_U be an $\mathbb{F}_q$-linear set of $\mathrm{PG}(r-1, q^n)$

$$\Omega \cap L_U = L_{U \cap W}.$$

O. Polverino

"Linear sets in projective spaces"

Discrete Math. 310(22) (2010), 3096-3107.

Intersection of two subgeometries

M. Svéd
"Baer subspaces in the n-dimensional projective space"
Lecture Notes in Math. 1036 (1983), 275-391.

I. Jagos, G. Kiss and A. Pór
"On the intersection of Baer subgeometries of $\mathrm{PG}(n, q^2)$"
Acta Sci. Math. 69(1-2) (2003), 419-429.

Intersection of two subgeometries

Let $L_{U_1} = \mathrm{PG}(r-1, p^{t_1})$ and $L_{U_2} = \mathrm{PG}(r-1, p^{t_2})$ contained in $\mathrm{PG}(r-1, q^n)$, with $q = p^h$, p prime $t_1 \leq t_2$.

If $L_{U_1} \cap L_{U_2} \neq \varnothing$, then

$$L_{U_1} \cap L_{U_2} = L_{W_1} \cup \ldots \cup L_{W_t},$$

where $L_{W_i} = \mathrm{PG}(s-1, p^m)$, $m = \gcd(t_1, t_2)$ and $t \leq \dfrac{q^n - 1}{p^{t_2} - 1}$.

G. Donati and N. Durante

"On the intersection of two subgeometries of $\mathrm{PG}(n, q)$"

Des. Codes Cryptogr. 46(3) (2008), 261-267.

Intersection of a subline with an $\mathbb{F}_q$-linear set

Let L_1 be an $\mathbb{F}_q$-linear set of $\mathrm{PG}(1,q^n)$ and let $L_2 = \mathrm{PG}(1,q^s)$ (with $s \mid n$) then either $L_1 \supseteq L_2$ or

$$|L_1 \cap L_2| \leq \frac{n}{s}(q^{s-1} + q^{s-2} + \ldots + 1)$$

V. Pepe
"On the algebraic variety $V_{r,t}$"
Finite Fields Appl. 17(4) (2011), 343-349.

M. Lavrauw and G. Van de Voorde
"On linear sets on a projective line"
Des. Codes Cryptogr. 56 (2010), 89-104.

Further cases

G. Donati and N. Durante
"Scattered linear sets generated by collineations between pencils of lines"
J. Algebr. Comb. 40(4) (2014), 1121-1134.

M. Lavrauw and G. Van de Voorde
"Scattered linear sets and pseudoreguli"
Electron. J. Combin. 20(1) (2013).

J. Sheekey, J.F. Voloch and G. Van de Voorde
"On the product of elements with prescribed trace"
arXiv:1910.09653 [Math.CO].

Our results

We consider $\mathbb{F}_q$-linear sets in $\mathrm{PG}(1,q^n)$ of rank n

Up to projectivity, every $\mathbb{F}_q$-linear set L in $\mathrm{PG}(1,q^n)$ of rank n can be written as follows

$$L = L_f = \{\langle (x, f(x))\rangle_{\mathbb{F}_{q^n}} : x \in \mathbb{F}_{q^n}^*\}$$

for some polynomial

$f(x) = a_0 x + \ldots + a_{n-1} x^{q^{n-1}} \in \mathbb{F}_{q^n}[x]$ (linearized polynomial)

Problem

Given two linearized polynomials f and g, then

$$|L_f \cap L_g| \geq 1?$$

Idea

$|L_f \cap L_g| \geq 1$ if and only if the curve

$$\mathscr{C} : \frac{f(X)}{X} - \frac{g(Y)}{Y} = 0$$

has at least one $\mathbb{F}_{q^n}$-rational affine point with nonzero coordinates

- Function fields theory
- Hasse-Weil bound

First analyzed case

Let $f(x) = \alpha x^q + \beta x \in \mathbb{F}_{q^n}[x]$

then L_f is an $\mathbb{F}_q$-linear set of rank n in $\mathrm{PG}(1,q^n)$ of pseudoregulus type

- MRD codes;
- Semifield theory;
- Blocking sets;
- etc...

First analyzed case

$$f(x) = \alpha x^q + \beta x \in \mathbb{F}_{q^n}[x]$$

$$g(x) = \sum_{i=0}^{n-1} a_i x^{q^i} \in \mathbb{F}_{q^n}[x]$$

The associated curve is

$$\mathscr{C} : X^{q-1} = \frac{g(Y) - \beta Y}{Y}$$

First analyzed case

The associated curve is

$$\mathscr{C}: X^{q-1} = \frac{g(Y) - \beta Y}{Y}$$

We then work in $\overline{\mathbb{F}_q}(y)$ ($\overline{\mathbb{F}_q}$ is the algebraic closure of $\mathbb{F}_q$) and we find an element of $\overline{\mathbb{F}_q}$ at which the valuation of $\dfrac{g(Y) - \beta Y}{Y}$ is coprime with $q-1 \Rightarrow \overline{\mathbb{F}_q}(x,y) : \overline{\mathbb{F}_q}(y)$ is a Kummer extension.

First analyzed case

The associated curve is

$$\mathscr{C} : X^{q-1} = \frac{g(Y) - \beta Y}{Y}$$

Then:

- $\mathscr{C}$ is absolutely irreducible
- We compute its genus (using the Kummer extension)
- We use Hasse-Weil bound to get the existence of a “good” point

$$f(x) = \alpha x^q + \beta x,\, g(x) = a_\ell x^{q^\ell} + a_{\ell_2} x^{q^{\ell_2}} + \ldots + a_d x^{q^d} \in \mathbb{F}_{q^n}[x]$$

Theorems [Zini and FZ-202x]

$g(y) = a_d y^{q^d}$

- If $\beta = 0$ then $L_f \cap L_g \neq \emptyset \Leftrightarrow \mathrm{N}_{q^n/q}(a_d/\alpha) = 1$
- If $\beta \neq 0$ and $d + 1 \leq n/2$ then $L_f \cap L_g \neq \emptyset$

$g(y) = a_d y^{q^d} + \beta y$

$$L_f \cap L_g \neq \emptyset \Leftrightarrow \mathrm{N}_{q^n/q}(a_d/\alpha) = 1$$

$$f(x) = \alpha x^q + \beta x, \; g(x) = a_\ell x^{q^\ell} + a_{\ell_2} x^{q^{\ell_2}} + \ldots + a_d x^{q^d} \in \mathbb{F}_{q^n}[x]$$

Theorem [Zini and FZ-202x]

In the remaining cases, let $m = \begin{cases} 0 & \text{if } a_0 \neq \beta \\ \ell & \text{if } a_0 = \beta = 0 \\ \ell_2 & \text{if } a_0 = \beta \neq 0 \end{cases}$

If $\max\{d+1-m, d/2\} \leq \begin{cases} n/2 & \text{if } m \leq d/2 \\ n/2 - 1 & \text{if } m > d/2 \end{cases}$ then

$$L_f \cap L_g \neq \emptyset$$

Second analyzed case

Let r_1 and r_2 such that $r_1, r_2 \mid n$ and $\gcd(r_1, r_2) = 1$ and let

$$f(x) = \mathrm{Tr}_{q^n/q^{r_1}}(x),\ g(x) = \alpha \mathrm{Tr}_{q^n/q^{r_2}}(x) \in \mathbb{F}_{q^n}[x]$$

$L_f, L_g \subseteq \mathrm{PG}(1,q^n)$

Clearly, the point $\langle (1,0) \rangle_{\mathbb{F}_{q^n}} \in L_f \cap L_g$.

So, the question is

When $|L_f \cap L_g| \geq 2$?

By Hilbert's 90 Theorem

We need to show the existence of an affine $\mathbb{F}_{q^n}$-rational point

$$\mathscr{D} : X^{q^{r_1}} - X - \frac{1}{\alpha}(Y^{q^{r_2}} - Y) + c = 0$$

By studying the above curve we get the following results.

Theorems [Zini and FZ-202x]

If there exists $a \in \mathbb{F}_{q^n}$ such that either

$\mathrm{Tr}_{q^n/q^{r_1}}(a) = -1$ and $\mathrm{Tr}_{q^n/q^{r_2}}(\alpha a) = 1$ or

$\mathrm{Tr}_{q^n/q^{r_1}}(a) = -1$ and $\mathrm{Tr}_{q^n/q^{r_2}}(a/\alpha) = 1$

then $|L_f \cap L_g| \geq 2$.

If $\alpha = ab$, with $a \in \mathbb{F}_{q^{r_1}}$ and $b \in \mathbb{F}_{q^{r_2}}$, then

$|L_f \cap L_g| \geq 2 \Leftrightarrow$

There exist $\gamma_1, \gamma_2 \in \mathbb{F}_{q^n}$ such that $\mathrm{Tr}_{q^n/q^{r_1}}(\gamma_1) = \mathrm{Tr}_{q^n/q^{r_2}}(\gamma_2) = 1$ and

$$\mathrm{Tr}_{q^n/q}\left(a\gamma_1 - \frac{\gamma_2}{b}\right) = 0.$$

Consider $L'_g = \{\langle(\alpha \mathrm{Tr}_{q^n/q^{r_2}}(x), x)\rangle_{\mathbb{F}_{q^n}} : x \in \mathbb{F}^*_{q^n}\}$

To study $L_f \cap L'_g$ we need the following curve

$$\frac{X}{\mathrm{Tr}_{q^n/q^{r_1}}(X)} \frac{Y}{\mathrm{Tr}_{q^n/q^{r_2}}(Y)} = \alpha$$

which can be replaced by

$$(U^{q^{r_1}} - U + \gamma_1)(V^{q^{r_2}} - V + \gamma_2) = \alpha$$

for some $\gamma_1, \gamma_2 \in \mathbb{F}_{q^n}$ such that $\mathrm{Tr}_{q^n/q^{r_1}}(\gamma_1) = \mathrm{Tr}_{q^n/q^{r_2}}(\gamma_2) = 1$

By using Artin-Schreier extensions and Hasse-Weil bound, we get the following result

Theorem [Zini and FZ-202x]

If $\dfrac{n}{2} \geq r_1 + r_2 + 1$, then $|L_f \cap L'_g| \geq 1$

Open problems

Open problems

- Investigate the intersection problem by choosing the polynomial $f(x)$ in a different family (Lunardon-Polverino linear sets, minimum size linear sets,…)

- To give more general conditions involving the parameters of a generic linear sets in $\mathrm{PG}(1,q^n)$

- How could we adapt these techniques for linear sets in $\mathrm{PG}(r,q^n)$ when $r \geq 2$?

Thank you for your attention!