European Journal of Combinatorics 114 (2023) 103792

Contents lists available at ScienceDirect

European Journal of Combinatorics

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

Renitent lines☆

Bence Csajbók[a,1], Peter Sziklai[a,b,c], Zsuzsa Weiner[a,d]

[a] ELKH–ELTE Geometric and Algebraic Combinatorics Research Group, ELTE Eötvös Loránd University, Department of Computer Science, 1117 Budapest, Pázmány P. stny. 1/C, Hungary
[b] ELTE Eötvös Loránd University, Budapest, Hungary, Department of Computer Science, 1117 Budapest, Pázmány P. stny. 1/C, Hungary
[c] Rényi Institute of Mathematics, 1053 Budapest, Reáltanoda u. 13-15, Hungary
[d] Prezi.com, Nagymező utca 54-56, H-1065 Budapest, Hungary

ARTICLE INFO

Article history:
Received 23 February 2021
Accepted 18 July 2023
Available online 18 August 2023

ABSTRACT

There are many examples for point sets in finite geometry which behave "almost regularly" in some (well-defined) sense, for instance they have "almost regular" line-intersection numbers. In this paper we investigate point sets of a desarguesian affine plane, for which there exist some (sometimes: many) parallel classes of lines, such that almost all lines of one parallel class intersect our set in the same number of points (possibly mod p, the characteristic). The lines with exceptional intersection numbers are called *renitent*, and we prove results on the (regular) behavior of these renitent lines. As a consequence of our results, we also prove geometric properties of codewords of the $\mathbb{F}_p$-linear code generated by characteristic vectors of lines of PG$(2, q)$.

☆ The first author was supported by the ÚNKP-19-4 New National Excellence Program of the Ministry for Innovation and Technology and by the National Research, Development and Innovation Office – NKFIH, Hungary, grant no. PD 132463. The first and the third author acknowledges the partial support of the National Research, Development and Innovation Office – NKFIH, Hungary, grant no. K 124950. The second author is grateful for the partial support of project K 120154 of the National Research, Development and Innovation Fund of Hungary; and for the support of the National Research, Development and Innovation Office, Hungary within the framework of the Thematic Excellence Program 2021 - National Research Subprogramme: "Artificial intelligence, large networks, data security: mathematical foundation and applications". This work was supported by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA–INdAM).

E-mail addresses: bence.csajbok@poliba.it (B. Csajbók), peter.sziklai@ttk.elte.hu (P. Sziklai), zsuzsa.weiner@gmail.com (Z. Weiner).

[1] Current address: Dipartimento di Meccanica, Matematica e Management, Politecnico di Bari, 70125 Bari, Via Orabona 4, Italy.

https://doi.org/10.1016/j.ejc.2023.103792
0195-6698/

1. Introduction

One of the key motivations in the history of finite geometries is the study of symmetric structures, i.e. structures admitting a large symmetry group. These structures (quadrics, Hermitian varieties, subgeometries over a subfield, etc.) are typically very "regular" when one considers their intersection properties with the subspaces of the ambient geometry; and there exist many "classification-type" results, stating that an "intersection-wise very regular" set must be one on the list of the (classical, symmetric) structures.

Throughout combinatorics, many theorems state that within a certain class of structures, the "nicest" ones (with respect to some well-defined combinatorial property) are *stable*, meaning that if another structure is "almost as nice", then that must be just a slightly modified version of a nicest one. Such *stability results*, as e.g. the Erdős–Simonovits theorem (see [1]) which states the stability of Turán's theorem in extremal graph theory, or the Hilton–Milner (see [2]) theorem for intersecting families, always describe some deep properties of the class.

Following this route, it is natural to investigate point sets, which behave "*almost* regularly" with respect to the subspaces of the ambient space. Describing the patterns how little irregularities may occur, reveals some properties of the regular structures.

In this paper we restrict ourselves to point sets of a desarguesian affine plane $\mathrm{AG}(2,q)$, where q is a power of the prime p. (The natural but not obvious extensions to other spaces will come in separate papers.) It may well happen that our point set intersects almost all lines of a parallel class in the same number of points, possibly mod p. (E.g. if you take a point set which intersects every line in constant mod p points and delete a few, say κ points of it then all the lines, except *at most* κ per parallel class, still intersect it in constant mod p points.) If it happens for many parallel classes, then one may guess that the reason is that our point set has a hidden structure, i.e. the non-regular intersections may be "corrected", or at least they also possess some regularity themselves. For instance, in $\mathrm{AG}(2,q)$, q even, an arc of size $q+1$ has almost regular intersection numbers mod 2 in every parallel line class: it meets each line in 0 or 2 points, except one line per each parallel class (which is 1-secant). Now, it is easy to prove that these 1-secant (exceptional) lines are concurrent, which can be interpreted as (i) they are *points of a degree* 1 *curve in the dual plane*; or (ii) their intersection point can be added to the original point set, which becomes "regular" this way (i.e. every line meets it in 0 mod 2 points). This tiny example illustrates that if you control the irregularities then you may prove that every oval is contained in a hyperoval (i.e. in the "nice structure"). In general, a $(q+2-k)$-arc is a point set (of size $(q+2-k)$) in $\mathrm{PG}(2,q)$ intersecting every line in at most 2 points. It is easy to see that such a point set has exactly k 1-secants through each of its point. Segre's celebrated theorem says that there is a curve of degree k or $2k$, depending on q is even or odd, in the dual plane which contains these 1-secants.

There are many papers dealing with problems in view of (ii), for a survey on arcs see [3] and for $k \pmod p$ multisets see [4]. In this paper we extend and explore this idea. We start with a result, which is from [5] and it can be viewed as a generalization of [6, Theorem 5], see also [7, Proposition 2] and [8, Remark 7]. We use the usual extension of $\mathrm{AG}(2,q)$ with its *line at infinity* ℓ_∞, containing points called *directions*, and the affine lines with slope d all meet at the direction (d), where $d \in \mathbb{F}_q \cup \{\infty\}$.

Lemma 1.1 (*Lemma of Renitent Lines [5]*)**.** *Let $\mathcal{T}$ be a point set of $\mathrm{AG}(2,q)$. A line ℓ with slope d is called renitent if there exists an integer m_d such that $|\ell \cap \mathcal{T}| \not\equiv m_d \pmod p$ but every other line with slope d meets $\mathcal{T}$ in m_d modulo p points. The renitent lines are concurrent.*

Now we define **renitent lines** in the following, more general setting and then prove various generalizations of the lemma above.

Definition 1.2. Let $\mathcal{T}$ be a multiset of $\mathrm{AG}(2,q)$. For some integer λ, a direction (d) is called $(q-\lambda)$-*uniform* w.r.t. $\mathcal{T}$ if there are at least $(q-\lambda)$ affine lines with slope d meeting $\mathcal{T}$ in the same number of points modulo p. This number will be called the *typical intersection number* at (d). The rest of the lines with direction (d) will be called *renitent* (w.r.t. $\mathcal{T}$).

A direction (d) is *sharply* $(q-\lambda)$-uniform w.r.t. $\mathcal{T}$ if it is incident with *exactly* $(q-\lambda)$ affine lines meeting $\mathcal{T}$ in the same number of points modulo p.

In the definition above, different directions might have different typical intersection numbers. In most cases we think about λ as a small value (hence the name *typical*), however in Theorems 2.1 and 2.4, in the prime case we do not need that λ is small. When q is non-prime we will usually suppose $\lambda \leq p-1$. In this latter case it is rather automatic that the typical intersection numbers are uniquely determined for each $(q-\lambda)$-uniform direction.

Remark 1.3. If $\lambda > (q-1)/2$ then it might happen that for a given $(q-\lambda)$-uniform direction (d) the typical intersection number is not uniquely determined. In this case one typical intersection number has to be fixed w.r.t. the direction (d).

Under some conditions, if a set of $(q-\lambda)$-uniform directions $\mathcal{E}_\lambda$ is of size at most q, then we are able to prove that the renitent lines are contained in an algebraic envelope of relatively small class (i.e. a curve of the dual plane of relatively small degree), see Theorem 2.1. This result resembles Segre's theorem mentioned above.

In Theorem 2.4, we remove the condition on the size of $\mathcal{E}_\lambda$ and give a more general formulation of Theorem 2.1. The proof relies on kth power sums and the Newton–Girard formulas. If we are more permissive with the renitent lines of $\mathcal{T}$ then the class of the algebraic envelope might increase. To prove the following result we apply a "weighted" version of the Newton–Girard formulas, see Lemma 3.1. The proof is given in Section 3, see Theorem 3.3.

Theorem 1.4. *Take a multiset $\mathcal{T}$ of $\mathrm{AG}(2,q)$ and an integer $0<\lambda\leq(q-1)/2$. Let $\mathcal{E}_\lambda$ denote a set of $(q-\lambda)$-uniform directions of size at most q. The renitent lines with slope in $\mathcal{E}_\lambda$ are contained in an algebraic envelope of class λ^2. Furthermore, if a direction is $(q-\lambda)$-uniform, but not sharply uniform, then the line pencil centered at that direction is fully contained in the envelope.*

In Section 4, we show how to apply the resultant method, cf. [4], with the help of a polynomial which can detect renitent lines at each uniform direction. For other polynomial techniques used in finite geometry, see for example [9]. In Section 5, we dualize some of our results and as a consequence, we also prove geometric properties of codewords of the $\mathbb{F}_p$-linear code generated by characteristic vectors of lines of $\mathrm{PG}(2,q)$. This is a generalization of a result of Blokhuis, Brouwer, Wilbrink [10, Proposition, p. 66].

2. Envelopes of small class

In this section our aim is to show that there is an *envelope* (i.e. a curve in the dual plane) of relatively small *class* (i.e. degree) containing the renitent lines with slope in a given subset $\mathcal{F}_\lambda$ of $(q-\lambda)$-uniform directions. There exist at least λ common lines of such an envelope and a line pencil centered at a sharply $(q-\lambda)$-uniform direction. So if there are $s>0$ sharply $(q-\lambda)$-uniform directions in $\mathcal{F}_\lambda$, then such an envelope has class at least $\min\{\lambda,s\}$ (if it has class less than λ then it necessarily contains the s line pencils centered at the sharply $(q-\lambda)$-uniform directions).

Any line set of size at most $|\mathcal{F}_\lambda|\lambda$ is contained in an algebraic envelope of class at most $\lceil\sqrt{2|\mathcal{F}_\lambda|\lambda}\rceil-1$. Indeed, a 3-variable homogeneous polynomial h of degree d has $\binom{d+2}{2}$ coefficients. For any point $P\in\mathrm{PG}(2,q)$, the condition that h vanishes at P is equivalent to a linear equation for these coefficients. If $\binom{d+2}{2}$ is larger than the size of a point set $\mathcal{S}$, then there is a non-trivial solution for the homogeneous system of equations which corresponds to the condition that the points of $\mathcal{S}$ are zeroes of h. In Theorem 2.1, we show that no matter of the size of $\mathcal{F}_\lambda$, with some conditions on the renitent lines we can always construct an envelope of class λ containing all renitent lines with slope in $\mathcal{F}_\lambda$. The results of this section will rely on the Newton–Girard formulas.

From now on, we coordinatize the projective plane $\mathrm{PG}(2,q)$ with homogeneous coordinates over $\mathrm{GF}(q)$ in such a way that the line at infinity is $[0:0:1]$, while the X- and the Y-axes are $[0:1:0]$ and $[1:0:0]$, resp. The direction (d), where $d\in\mathbb{F}_q$, means the point $(1:d:0)$ on the line at infinity.

Later in this section, we will be able to remove the condition $|\mathcal{E}_\lambda|\leq q$ from Theorem 2.1, see Remark 2.5.

Theorem 2.1. *Take a multiset $\mathcal{T}$ of* AG$(2,q)$ *and let $\mathcal{E}_\lambda$ denote a set of $(q-\lambda)$-uniform directions of size at most q such that:*

(i) $0 < \lambda \le \min\{q-2, p-1\}$,
(ii) *for each $(d) \in \mathcal{E}_\lambda$ the renitent lines meet $\mathcal{T}$ in the same number, say t_d, of points modulo p,*
(iii) *for each $(d) \in \mathcal{E}_\lambda$ if m_d denotes the typical intersection number at direction (d), then $t_d - m_d$ modulo p does not depend on the choice of (d).*

Then the renitent lines with direction in $\mathcal{E}_\lambda$ are contained in an algebraic envelope of class λ.

Proof. First we show that the number of renitent lines is the same at each direction (d) of $\mathcal{E}_\lambda$, hence we can find a common value $\lambda' \le \lambda$ for which all the directions in $\mathcal{E}_\lambda$ are sharply $(q-\lambda')$-uniform; note that if $\lambda' < \lambda$ then we will find an envelope of even smaller class at the end of the proof. Let (d) and (e) denote two directions in $\mathcal{E}_\lambda$ which are sharply $(q-\lambda_d)$-uniform and sharply $(q-\lambda_e)$-uniform, respectively. Then, counting points on lines with slope d and lines with slope e, we obtain

$$(q-\lambda_d)m_d + \lambda_d t_d \equiv |\mathcal{T}| \equiv (q-\lambda_e)m_e + \lambda_e t_e \pmod p,$$

hence

$$\lambda_d(t_d - m_d) \equiv \lambda_e(t_e - m_e) \pmod p.$$

By assumption *(iii)*, $t_d - m_d \equiv t_e - m_e \pmod p$ and $t_d \not\equiv m_d \pmod p$, thus $\lambda_d \equiv \lambda_e \pmod p$. Then $\lambda_d = \lambda_e$ follows from the fact that $0 \le \lambda_e, \lambda_d \le \lambda \le p-1$.

From now on, we may assume that we had $\lambda = \lambda'$ already, and the directions in $\mathcal{E}_\lambda$ are sharply $(q-\lambda)$-uniform. Since $|\mathcal{E}_\lambda| \le q$, we may assume $(0:1:0) \notin \mathcal{E}_\lambda$. For each $(1:d:0) \in \mathcal{E}_\lambda$ put $(0:\alpha_1(d):1), (0:\alpha_2(d):1), \dots, (0:\alpha_\lambda(d):1)$ for the points of the Y-axis on the renitent lines with slope d.

Put $s := |\mathcal{T}|$ and $\mathcal{T} = \{(a_i:b_i:1)\}_{i=1}^s$. Next define the polynomials

$$\pi_k(V) := \sum_{i=1}^{s} (b_i - a_i V)^k \in \mathbb{F}_q[V]$$

of degree at most k. We project $\mathcal{T}$ from (d) to the Y-axis: the line joining $(1:d:0)$ and $(a_i:b_i:1)$ meets the Y-axis at the point $(0:b_i - a_i d:1)$, hence for each $(1:d:0) \in \mathcal{E}_\lambda$ the projected image, i.e. the multiset

$$M_d := \{(b_i - a_i d)\}_{i=1}^s$$

contains $m_d \bmod p$ copies of the values belonging to non-renitent lines and $t_d \bmod p$ copies of the $\alpha_i(d)$'s, or one may say $m_d \bmod p$ copies of $\mathbb{F}_q$ and $c \bmod p$ further copies of $\alpha_i(d)$ for $1 \le i \le \lambda$, where $c \in \{1, \dots, p-1\}$ is an integer such that $c \equiv t_d - m_d \pmod p$. Since $\sum_{\gamma \in \mathbb{F}_q} \gamma^k = 0$ for $0 \le k \le q-2$ and since $\pi_k(d)$ is the kth power sum of the elements in M_d, for $0 \le k \le q-2$ it holds that for $(1:d:0) \in \mathcal{E}_\lambda$

$$\pi_k(d) = c \sum_{i=1}^{\lambda} \alpha_i(d)^k. \tag{1}$$

Denote by $\sigma_i(X_1, \dots, X_\lambda)$ the ith elementary symmetric polynomial in the variables $X_1, \dots, X_\lambda$. Also, for any integer $i \ge 0$ and $d \in \mathcal{E}_\lambda$ put

$$\sigma_i(d) = \sigma_i(\alpha_1(d), \dots, \alpha_\lambda(d)).$$

For $p-1 \ge j \ge 1$ define the following polynomial of degree at most j:

$$S_j(V) := (-1)^j \sum_{\substack{n_1+2n_2+\cdots+jn_j=j \\ n_1,n_2,\dots,n_j \ge 0}} \prod_{i=1}^{j} \frac{(-\pi_i(V)/c)^{n_i}}{n_i! i^{n_i}} \in \mathbb{F}_q[V].$$

Then for $\min\{q-2, p-1\} \geq j \geq 1$ from (1) and from the Newton–Girard identities it follows that $S_j(d) = \sigma_j(d)$ for each $(1 : d : 0) \in \mathcal{E}_\lambda$.

Consider the affine curve of degree λ defined by

$$f(U,V) := U^\lambda - S_1(V)U^{\lambda-1} + S_2(V)U^{\lambda-2} - \cdots + (-1)^{\lambda-1}S_{\lambda-1}(V)U + (-1)^\lambda S_\lambda(V).$$

Then the projective curve of degree λ defined by the equation $g(U,V,W) := W^\lambda f(U/W, V/W)$ contains the point $(\alpha_i(d) : d : 1)$ for each $d \in \mathcal{E}_\lambda$ and $1 \leq i \leq \lambda$. Indeed,

$$g(U,d,1) = U^\lambda - \sigma_1(d)U^{\lambda-1} + \sigma_2(d)U^{\lambda-2} - \cdots + (-1)^{\lambda-1}\sigma_{\lambda-1}(d)U + (-1)^\lambda\sigma_\lambda(d) =$$

$$\prod_{i=1}^{\lambda}(U - \alpha_i(d)).$$

It follows that the lines $[d : -1 : \alpha_i(d)]$ are contained in an algebraic envelope of class λ. □

Let U be an affine $(q-n)$-set and denote by D_U the set of directions determined by U (that is, directions incident with at least one line meeting U in at least 2 points). Szőnyi proved in [8, Theorem 4] that the affine lines which do not meet U and are incident with a not determined direction are contained in an algebraic envelope of class n. If $\lambda \leq \min\{q-2, p-1\}$, then this is a special case of our Theorem 2.1, with $\lambda = n$, $\mathcal{E}_n = \ell_\infty \setminus D_U$ (for $d \in \mathcal{E}_n$ it holds that $t_d = 0$ and $m_d = 1$). To construct the envelope, Szőnyi's proof relies on the fact that a typical line intersects U in 1 point exactly, while a renitent line in 0 point. Our theorem considers a more general setting, but the cost of it is that we need an upper bound on λ.

As in [8], if $\lambda \leq \sqrt{q}/2$ and $|\mathcal{E}_\lambda| \geq (q+1)/2$, then [8, Proposition 2] yields that the envelope constructed in Theorem 2.1 is the product of n pencils. (For an improved version of [8, Proposition 2] see [11, Lemma 3.2].) This actually happens as the next example shows.

Example 2.2. In AG$(2,q)$ consider an m mod p multiset and remove λ of its points. These λ points determine at most $\binom{\lambda}{2}$ directions which we will denote by D. Then the points of $\ell_\infty \setminus D$ are $(q-\lambda)$-uniform with typical intersection number m and the renitent lines (lines meeting U in $m-1$ mod p points) are contained in the product of the λ pencils centered at the removed points.

As the next example shows, Theorem 2.1 does not hold when $\lambda = p^2 - p$, hence we certainly need some restriction on the value λ. In Section 5, we show that the bound $\lambda \leq p-1$ is necessary when $q = p^2$.

Example 2.3. In AG$(2,q)$, $q = p^h$, p prime, $h > 2$, consider a subplane PG$(2,p)$ and delete $p+1$ collinear points from it. Let $\mathcal{T}$ denote the point set obtained, $\mathcal{T} = \{Q_1, Q_2, \ldots, Q_{p^2}\}$. Denote by $P_1, \ldots, P_{p^2+p}$ the points of ℓ_∞ through which there passes a p-secant of $\mathcal{T}$. These points are incident with p^2-p affine lines meeting $\mathcal{T}$ in 1 point and with $q-p^2+p$ affine lines meeting $\mathcal{T}$ in 0 modulo p points.

We claim that the $(p^2+p)(p^2-p)$ renitent lines are not contained in an envelope of class p^2-p. Indeed, the point Q_i is incident with $p^2+p-(p+1)$ lines containing a point P_j for some $j \in [1, p^2+p]$ and intersecting $\mathcal{T}$ in 1 modulo p points, i.e with this many renitent lines; so the pencil with center Q_i would be a component of such an envelope for each i. A contradiction by degree considerations.

The next theorem seems to have rather artificial conditions and settings. But this provides a middle ground between the kind of best bound deg $\leq \lambda$ of Theorem 2.1 with strong assumptions and the weaker bound deg $\leq \lambda^2$ of Theorem 3.3 holding in general.

Theorem 2.4. *Take a multiset $\mathcal{T}$ of AG$(2,q)$ and let $\mathcal{F}_\lambda$ denote a set of $(q-\lambda)$-uniform directions. For each $(d) \in \mathcal{F}_\lambda$ denote the typical intersection number by m_d and denote the intersection numbers of the renitent lines by $t_{d,1}, t_{d,2}, \ldots, t_{d,\lambda_d}$, for some $0 < \lambda_d \leq \lambda$. For $c \in \mathbb{F}_p \setminus \{0\}$ define the integers $\lambda_{d,i}(c) \in \{1, \ldots, p-1\}$ such that*

$$c\lambda_{d,i}(c) \equiv t_{d,i} - m_d \pmod p$$

and assume that

$$\Lambda_d(c) := \sum_{i=1}^{\lambda_d} \lambda_{d,i}(c) \le \min\{q-2, p-1\} \tag{2}$$

holds for each $(d) \in \mathcal{F}_\lambda$ *(note that the sum is taken over natural numbers). Then* $\Lambda(c) := \Lambda_d(c)$ *does not depend on* d *and the renitent lines with direction in* $\mathcal{F}_\lambda$ *are contained in an algebraic envelope of class* $\Lambda(c)$*. If* ℓ *is a renitent line with slope* d *and with intersection number* $t_{d,i}$*, then the intersection multiplicity of the pencil centered at* (d) *with* $\mathcal{F}_\lambda$ *at* ℓ *is* $\lambda_{d,i}(c)$*.*

Proof. Throughout the proof, we will fix c and so neglect it from $\lambda_{d,i}(c)$, $\Lambda_d(c)$ and $\Lambda(c)$. As before, first we show that Λ_d does not depend on (d) of $\mathcal{F}_\lambda$. Let (e_1) and (e_2) denote two directions in $\mathcal{F}_\lambda$. Then

$$qm_{e_1} + \Lambda_{e_1} c \equiv |\mathcal{T}| \equiv qm_{e_2} + \Lambda_{e_2} c \pmod p,$$

hence

$$\Lambda_{e_1} \equiv \Lambda_{e_2} \pmod p.$$

Then $\Lambda_{e_1} = \Lambda_{e_2}$ follows from the fact that $0 < \Lambda_{e_1}, \Lambda_{e_2} \le p-1$.

First we prove the assertion for any $\mathcal{E}_\lambda \subseteq \mathcal{F}_\lambda$ such that $|\mathcal{E}_\lambda| \le q$. In this case, we may assume $(0:1:0) \notin \mathcal{E}_\lambda$. For each $(1:d:0) \in \mathcal{E}_\lambda$ put $(0:\alpha_1(d):1), (0:\alpha_2(d):1), \dots, (0:\alpha_{\lambda_d}(d):1)$ for the points of the Y-axis on the renitent lines with slope d.

Put $s := |\mathcal{T}|$ and $\mathcal{T} = \{(a_i : b_i : 1)\}_{i=1}^s$. Next define the polynomials

$$\pi_k(V) := \sum_{i=1}^{s} (b_i - a_i V)^k \in \mathbb{F}_q[V]$$

of degree at most k. For each $(1:d:0) \in \mathcal{E}_\lambda$ the multiset

$$M_d := \{(b_i - a_i d)\}_{i=1}^s$$

contains m_d modulo p copies of $\mathbb{F}_q$ and $t_{d,i} - m_d$ modulo p further copies of $\alpha_i(d)$ for $1 \le i \le \lambda_d$. Since $\sum_{\gamma \in \mathbb{F}_q} \gamma^k = 0$ for $0 \le k \le q-2$ and since $\pi_k(d)$ is the kth power sum of the elements in M_d, for $0 \le k \le q-2$ it holds that for $(1:d:0) \in \mathcal{E}_\lambda$

$$\pi_k(d) = c \sum_{i=1}^{\lambda_d} \sum_{j=1}^{\lambda_{d,i}} \alpha_i(d)^k. \tag{3}$$

Denote by $\sigma_i(X_1, \dots, X_\Lambda)$ the ith elementary symmetric polynomial in the variables $X_1, \dots, X_\Lambda$. Also, for any integer $i \ge 0$ and $d \in \mathcal{E}_\lambda$ put

$$\sigma_i(d) = \sigma_i(\underbrace{\alpha_1(d), \dots, \alpha_1(d)}_{\lambda_{d,1} \text{ times}}, \dots, \underbrace{\alpha_j(d), \dots, \alpha_j(d)}_{\lambda_{d,j} \text{ times}}, \dots, \underbrace{\alpha_{\lambda_d}(d), \dots, \alpha_{\lambda_d}(d)}_{\lambda_{d,\lambda_d} \text{ times}}).$$

For $p-1 \ge j \ge 1$ define the following polynomial of degree at most j:

$$S_j(V) := (-1)^j \sum_{\substack{n_1+2n_2+\cdots+jn_j=j \\ n_1,n_2,\dots,n_j \ge 0}} \prod_{i=1}^{j} \frac{(-\pi_i(V)/c)^{n_i}}{n_i! i^{n_i}} \in \mathbb{F}_q[V].$$

Then for $\min\{q-2, p-1\} \ge j \ge 1$ from (3) and from the Newton–Girard identities it follows that $S_j(d) = \sigma_j(d)$ for each $(1:d:0) \in \mathcal{E}_\lambda$.

Consider the affine curve of degree Λ defined by

$$f(U,V) := U^\Lambda - S_1(V)U^{\Lambda-1} + S_2(V)U^{\Lambda-2} - \cdots + (-1)^{\Lambda-1} S_{\Lambda-1}(V)U + (-1)^\Lambda S_\Lambda(V).$$

Then the projective curve of degree Λ defined by the equation $g(U,V,W) := W^{\Lambda} f(U/W, V/W)$ contains the point $(\alpha_i(d) : d : 1)$ for each $d \in \mathcal{E}_\lambda$ and $1 \le i \le \lambda_d$, with multiplicity $\lambda_{d,i}$. Indeed,

$$g(U,d,1) = U^{\Lambda} - \sigma_1(d)U^{\Lambda-1} + \sigma_2(d)U^{\Lambda-2} - \cdots + (-1)^{\Lambda-1}\sigma_{\Lambda-1}(d)U + (-1)^{\Lambda}\sigma_{\Lambda}(d) =$$

$$\prod_{i=1}^{\lambda_d}(U - \alpha_i(d))^{\lambda_{d,i}}.$$

It follows that the point $(\alpha_i(d) : d : 1)$ lies on the curve defined by g. Note that $(V - d)$ cannot divide $f(U,V)$ and hence the "horizontal" line $[0 : 1 : -d]$ cannot be a component of the curve defined by f. The intersection multiplicity of the curve defined by f and $[0 : 1 : -d]$ is $\lambda_{d,i}$ at the point $(\alpha_i(d) : d : 1)$. It follows that the lines $[d : -1 : \alpha_i(d)]$ are contained in an algebraic envelope of class Λ and the intersection multiplicity of this envelope with the pencil centered at $(1 : d : 0)$ is $\lambda_{d,i}$ at the line $[d : -1 : \alpha_i(d)]$.

Now assume that $|\mathcal{F}_\lambda| = q+1$. Apply the argument above for two distinct subsets of $\mathcal{F}_\lambda$, both of them of size q. Denote them by $\mathcal{E}_\lambda$ and $\mathcal{E}'_\lambda$ and denote the corresponding curves (in the dual plane) of degree Λ by $\mathcal{C}$ and $\mathcal{C}'$, respectively. Our aim is to prove that these two curves coincide. Put $\mathcal{C} = \mathcal{H} \cdot \mathcal{A}$ and $\mathcal{C}' = \mathcal{H} \cdot \mathcal{A}'$, where $\mathcal{A}$ and $\mathcal{A}'$ do not have a common component. Denote the degree of $\mathcal{H}$ by h and suppose to the contrary that $h < \Lambda$.

For $(d) \in \mathcal{E}_\lambda \cap \mathcal{E}'_\lambda$ denote the line $[0 : 1 : -d]$ by ℓ_d and the point $(\alpha_i(d) : d : 1)$ by $P_{d,i}$. Recall that ℓ_d cannot be a component of $\mathcal{C}$ or $\mathcal{C}'$. The intersection multiplicity $\mathrm{I}(\mathcal{C} \cap \ell_d, P_{d,i}) = \lambda_{d,i}$ equals $\mathrm{I}(\mathcal{H} \cap \ell_d, P_{d,i}) + \mathrm{I}(\mathcal{A} \cap \ell_d, P_{d,i})$, thus

$$\mathrm{I}(\mathcal{A} \cap \ell_d, P_{d,i}) = \lambda_{d_i} - \mathrm{I}(\mathcal{H} \cap \ell_d, P_{d,i}).$$

Replacing $\mathcal{A}$ by $\mathcal{A}'$, the same argument yields that

$$\mathrm{I}(\mathcal{A}' \cap \ell_d, P_{d,i}) = \lambda_{d_i} - \mathrm{I}(\mathcal{H} \cap \ell_d, P_{d,i}).$$

By [12, Lemma 9.2 and p. 87] or [13, Lemma 10.4] it follows that $\mathrm{I}(\mathcal{A} \cap \mathcal{A}', P_{d,i}) \ge \lambda_{d_i} - \mathrm{I}(\mathcal{H} \cap \ell_d, P_{d,i})$. Then

$$\sum_{i=1}^{\lambda_d} \mathrm{I}(\mathcal{A} \cap \mathcal{A}', P_{d,i}) \ge \sum_{i=1}^{\lambda_d} \lambda_{d_i} - \sum_{i=1}^{\lambda_d} \mathrm{I}(\mathcal{H} \cap \ell_d, P_{d,i}) = \Lambda - \sum_{i=1}^{\lambda_d} \mathrm{I}(\mathcal{H} \cap \ell_d, P_{d,i}) \ge \Lambda - h, \tag{4}$$

since $\sum_{i=1}^{\lambda_d} \mathrm{I}(\mathcal{H} \cap \ell_d, P_{d,i}) \le \deg \mathcal{H} = h$. The inequality (4) holds for each $(d) \in \mathcal{E}_\lambda \cap \mathcal{E}'_\lambda$ and hence

$$\sum_{P \in \mathcal{A} \cap \mathcal{A}'} \mathrm{I}(\mathcal{A} \cap \mathcal{A}', P) \ge \sum_{(d) \in \mathcal{E}_\lambda \cap \mathcal{E}'_\lambda} \sum_{i=1}^{\lambda_d} \mathrm{I}(\mathcal{A} \cap \mathcal{A}', P_{d,i}) \ge (q-1)(\Lambda - h).$$

On the other hand, By Bézout's theorem $\sum_{P \in \mathcal{A} \cap \mathcal{A}'} \mathrm{I}(\mathcal{A} \cap \mathcal{A}', P) \le \deg \mathcal{A} \cdot \deg \mathcal{A}' = (\Lambda - h)(\Lambda - h)$.

This contradiction proves $h = \Lambda$, that is, $\mathcal{C} = \mathcal{C}'$. □

Remark 2.5. If in Theorem 2.4 we assume $t_{d,1} = t_{d,2} = \cdots = t_{d,\lambda_d} =: t_d$ for each $(d) \in \mathcal{F}_\lambda$, we also assume that $t_d - m_d$ does not depend on the choice of d, and further assume $0 < \lambda \le \min\{q-2, p-1\}$, then with the choice $c \equiv t_d - m_d \pmod p$ we obtain Theorem 2.1 without the restriction $|\mathcal{E}_\lambda| \le q$.

Remark 2.6. If $|\mathcal{T}| \equiv 0 \pmod p$ then Theorem 2.4 cannot be applied. Indeed, in that case for each $(d) \in \mathcal{F}_\lambda$,

$$\sum_{i=1}^{\lambda_d}(t_{d,i} - m_d) \equiv 0 \pmod p$$

and hence $\Lambda_d = \sum_{i=1}^{\lambda_d} \lambda_{d,i} \equiv 0 \pmod p$, which is not possible if $\Lambda_d \le p-1$ (by definition $\lambda_{d,i} > 0$ for each i).

Remark 2.7. For $c = 1, 2, \dots, p-1$, the values of $\Lambda_d(c)$ give different residues modulo p and this residue is the same for every choice of d. However, it is possible that for some of the directions, $\Lambda_d(c) \le \min\{q-2, p-1\}$ does not hold.

Indeed, put for example $p = 5$, $\lambda = 2$ and assume that the typical intersection number is 0 at each direction. Also, assume that both of the two renitent lines with direction $(d_1) \in \mathcal{F}_\lambda$ meet $\mathcal{T}$ in 1 modulo p points and the two renitent lines with direction $(d_2) \in \mathcal{F}_\lambda$ meet $\mathcal{T}$ in 3 and in 4 points modulo p. Then, with $c = 1$ we obtain $\Lambda_{d_1}(c) = 2$ and $\Lambda_{d_2}(c) = 7$, so the result cannot be applied. On the other hand, with $c = 3$ we obtain $\Lambda_{d_1}(c) = \Lambda_{d_2}(c) = 4$ and hence the result can be applied if $q > 5$. This also shows that sometimes it might be convenient to choose $\mathcal{F}_\lambda$ not as the set of all $(q-\lambda)$-uniform directions, but as a subset of them.

Example 2.8. In Theorem 2.4, put $\lambda = 3$ and assume that $m_d = 1$ and the renitent lines meet $\mathcal{T}$ modulo p in the multiset $\{3, 3, 5\}$ for each $(d) \in \mathcal{F}_\lambda$. Note that this implies $p \neq 2$. With the choice $c = 2$, it follows that the renitent lines are contained in a curve of degree $\Lambda = (3-1)/2 + (3-1)/2 + (5-1)/2 = 4$ whenever $4 \le \min\{q-2, p-1\}$.

One might think that to obtain a curve of the lowest degree, the best option is to chose c as the greatest common divisor of the values $t_{d,i} - m_d$. The next example disproves this belief.

Example 2.9. In Theorem 2.4, put $\lambda = 2$, $p = 13$, and assume that $m_d = 1$ and the renitent lines meet $\mathcal{T}$ modulo 13 in the set $\{2, 8\}$ for each $(d) \in \mathcal{F}_\lambda$. With the choice $c = 1$, it follows that the renitent lines are contained in a curve of degree $\Lambda = (2-1) + (8-1) = 8$. With the choice $c = 7$, it follows that the renitent lines are contained in a curve of degree $\Lambda = 1/7 + 7/7 = 2 + 1 = 3$.

3. The general case

First we prove a recursion connecting elementary symmetric polynomials with "weighted" power sums.

Lemma 3.1. *Let $\sigma_k = \sigma_k(X_1, \dots, X_\lambda)$ denote the kth elementary symmetric polynomial in the variables $X_1, \dots, X_\lambda$. For some field elements $c_1, c_2, \dots, c_\lambda$ put*

$$P_k = P_k(X_1, \dots, X_\lambda) = \sum_{i=1}^{\lambda} c_i X_i^k.$$

Then for any integer $j \ge 0$ it holds that

$$P_{\lambda+j} = P_{\lambda+j-1}\sigma_1 - P_{\lambda+j-2}\sigma_2 + \cdots + (-1)^{\lambda+1} P_j \sigma_\lambda.$$

Proof. Note that

$$Y^j \prod_{i=1}^{\lambda} (Y - X_i) = Y^{\lambda+j} - Y^{\lambda+j-1}\sigma_1 + Y^{\lambda+j-2}\sigma_2 - \cdots + (-1)^\lambda Y^j \sigma_\lambda.$$

It follows that

$$c_1(X_1^{\lambda+j} - X_1^{\lambda+j-1}\sigma_1 + X_1^{\lambda+j-2}\sigma_2 - \cdots + (-1)^\lambda X_1^j \sigma_\lambda) = 0,$$

$$c_2(X_2^{\lambda+j} - X_2^{\lambda+j-1}\sigma_1 + X_2^{\lambda+j-2}\sigma_2 - \cdots + (-1)^\lambda X_2^j \sigma_\lambda) = 0,$$

$$\vdots$$

$$c_\lambda(X_\lambda^{\lambda+j} - X_\lambda^{\lambda+j-1}\sigma_1 + X_\lambda^{\lambda+j-2}\sigma_2 - \cdots + (-1)^\lambda X_\lambda^j \sigma_\lambda) = 0.$$

Summing up both sides above yields the assertion. □

Lemma 3.2. *As before, put*

$$P_k = P_k(X_1, \dots, X_\lambda) = \sum_{i=1}^{\lambda} c_i X_i^k,$$

and define the $\lambda \times \lambda$ matrix

$$H = H(X_1, \dots, X_\lambda) = \begin{pmatrix} P_{\lambda-1} & P_{\lambda-2} & \dots & P_0 \\ P_\lambda & P_{\lambda-1} & \dots & P_1 \\ \vdots & \vdots & \vdots & \vdots \\ P_{2\lambda-2} & P_{2\lambda-3} & \dots & P_{\lambda-1} \end{pmatrix}.$$

Then $\det H = (-1)^{\lambda(\lambda-1)/2} c_1 c_2 \dots c_\lambda \prod_{1 \le i < j \le \lambda} (X_i - X_j)^2$.

Proof. It follows from the properties of Vandermonde matrices and from the fact that

$$H = \begin{pmatrix} c_1 & c_2 & \dots & c_\lambda \\ c_1 X_1 & c_2 X_2 & \dots & c_\lambda X_\lambda \\ \vdots & & & \\ c_1 X_1^{\lambda-1} & c_2 X_2^{\lambda-1} & \dots & c_\lambda X_\lambda^{\lambda-1} \end{pmatrix} \begin{pmatrix} X_1^{\lambda-1} & X_1^{\lambda-2} & \dots & 1 \\ X_2^{\lambda-1} & X_2^{\lambda-2} & \dots & 1 \\ \vdots & & & \\ X_\lambda^{\lambda-1} & X_\lambda^{\lambda-2} & \dots & 1 \end{pmatrix}. \quad \square$$

Now we are ready to prove an upper bound for the degree of the curve, under very general conditions.

Theorem 3.3. *Take a multiset $\mathcal{T}$ of* AG$(2, q)$ *and an integer $0 < \lambda \le (q-1)/2$. Let $\mathcal{E}_\lambda$ denote a set of $(q-\lambda)$-uniform directions of size at most q and assume that there is at least one sharply $(q-\lambda)$-uniform direction in $\mathcal{E}_\lambda$. Then the renitent lines with slope in $\mathcal{E}_\lambda$ are contained in an algebraic envelope of class λ^2 with the following properties:*

(1) if a direction (u) of $\mathcal{E}_\lambda$ is $(q-\lambda_u)$-uniform for some $0 \le \lambda_u < \lambda$ then the line pencil centered at (u) is fully contained with multiplicity $(\lambda - \lambda_u)$ in the envelope;
(2) pencils centered at sharply $(q-\lambda)$-uniform directions are not contained in the envelope.

Proof. For each $(1 : d : 0) \in \mathcal{E}_\lambda$ denote by λ_d the number of renitent lines with slope d and denote by $(0 : \alpha_1(d) : 1), (0 : \alpha_2(d) : 1), \dots, (0 : \alpha_{\lambda_d}(d) : 1)$ the points of the Y-axis on these lines (first we assume $\lambda_d > 0$, the $\lambda_d = 0$ case is very simple and it is treated in the last paragraph of the proof). Also, denote the typical intersection number at (d) by m_d. Put $s := |\mathcal{T}|$ and $\mathcal{T} = \{(a_i : b_i : 1)\}_{i=1}^s$. Next define the polynomials

$$\pi_k(V) := \sum_{i=1}^{s} (b_i - a_i V)^k \in \mathbb{F}_q[V]$$

of degree at most k. As in the earlier proofs, for any $(1 : d : 0) \in \mathcal{E}_\lambda$ the multiset

$$M_d := \{(b_i - a_i d)\}_{i=1}^s$$

contains m_d modulo p copies of $\mathbb{F}_q$ and $c_i(d) \not\equiv 0$ modulo p further copies of $\alpha_i(d)$ for $1 \le i \le \lambda_d$. Since $\sum_{g \in \mathbb{F}_q} g^k = 0$ for $0 \le k \le q-2$ and since $\pi_k(d)$ is the kth power sum of M_d, for $0 \le k \le q-2$ it holds that

$$\pi_k(d) = \sum_{i=1}^{\lambda_d} c_i(d) \alpha_i(d)^k. \tag{5}$$

Note that $\pi_k(d)$ is as $P_k(\alpha_1(d), \alpha_2(d), \dots, \alpha_{\lambda_d}(d))$ (with $c_i = c_i(d)$) in Lemma 3.1. For any integer $i \ge 0$ and $(1 : d : 0) \in \mathcal{E}_\lambda$ put

$$\sigma_i(d) = \sigma_i(\alpha_1(d), \dots, \alpha_{\lambda_d}(d)),$$

where for $i > \lambda_d$ we define $\sigma_i(d)$ to be 0.

For $j \geq 0$, $q-2 \geq \lambda_d + j$ and $(1:d:0) \in \mathcal{E}_\lambda$ Lemma 3.1 yields

$$\pi_{\lambda_d+j}(d) = \pi_{\lambda_d+j-1}(d)\sigma_1(d) - \pi_{\lambda_d+j-2}(d)\sigma_2(d) + \cdots + (-1)^{\lambda_d+1}\pi_j(d)\sigma_{\lambda_d}(d). \tag{6}$$

Define

$$H(V) = \begin{pmatrix} \pi_{\lambda-1}(V) & \pi_{\lambda-2}(V) & \dots & \pi_0(V) \\ \pi_\lambda(V) & \pi_{\lambda-1}(V) & \dots & \pi_1(V) \\ \vdots & \vdots & \vdots & \vdots \\ \pi_{2\lambda-2}(V) & \pi_{2\lambda-3}(V) & \dots & \pi_{\lambda-1}(V) \end{pmatrix}.$$

Then for each $(1:d:0) \in \mathcal{E}_\lambda$, since $2\lambda - 1 \leq q-2$, by (6) applied for $\lambda - \lambda_d \leq j \leq 2\lambda - \lambda_d - 1$, we obtain

$$H(d)\begin{pmatrix} \sigma_1(d) \\ -\sigma_2(d) \\ \vdots \\ (-1)^{\lambda+1}\sigma_\lambda(d) \end{pmatrix} = \begin{pmatrix} \pi_\lambda(d) \\ \pi_{\lambda+1}(d) \\ \vdots \\ \pi_{2\lambda-1}(d) \end{pmatrix}. \tag{7}$$

Denote by $H_i(V)$ the matrix obtained from $H(V)$ by replacing its ith column with

$$C(V) := (\pi_\lambda(V), \pi_{\lambda+1}(V), \dots, \pi_{2\lambda-1}(V))^T.$$

Put $S(V) = \det H(V)$ and $S_i(V) = \det H_i(V)$. Then $\deg S \leq \lambda(\lambda-1)$ and $\deg S_i(V) \leq \lambda^2 - \lambda + i$. Also, $S(d) = \det H(d)$ and $S_i(d) = \det H_i(d)$ for $(1:d:0) \in \mathcal{E}_\lambda$. Consider the affine curve $\mathcal{C}$ of degree at most λ^2 defined by the equation

$$f(U,V) := S(V)U^\lambda - S_1(V)U^{\lambda-1} - S_2(V)U^{\lambda-2} - \cdots - S_{\lambda-1}(V)U - S_\lambda(V). \tag{8}$$

By Lemma 3.2, if $(1:d:0) \in \mathcal{E}_\lambda$ is sharply $(q-\lambda)$-uniform, then the determinant of $H(d)$ is $(-1)^{\lambda(\lambda-1)/2}\prod_{i=1}^{\lambda} c_i(d)\prod_{1\leq i<j\leq\lambda}(\alpha_i(d)-\alpha_j(d))^2$ and hence $H(d)$ is invertible and the existence of a sharply $(q-\lambda)$-uniform direction ensures that $S(V)$ is not the zero-polynomial. Then by Cramer's rule $(-1)^{i+1}\sigma_i(d) = \det H_i(d)/\det H(d) = S_i(d)/S(d)$ for $1 \leq i \leq \lambda$.

Hence if $(1:d:0) \in \mathcal{E}_\lambda$ is sharply $(q-\lambda)$-uniform (that is $\lambda_d = \lambda$), then $(\alpha_i(d), d)$ is a point of $\mathcal{C}$ defined in (8) for each $1 \leq i \leq \lambda_d$, since in this case $f(U,d)$ equals

$$S(d)(U^\lambda - \sigma_1(d)U^{\lambda-1} + \sigma_2(d)U^{\lambda-2} - \cdots + (-1)^{\lambda-1}\sigma_{\lambda-1}(d)U + (-1)^\lambda\sigma_\lambda(d)) =$$

$$S(d)\prod_{i=1}^{\lambda}(U - \alpha_i(d)).$$

Now consider $(1:d:0) \in \mathcal{E}_\lambda$ such that $\lambda_d < \lambda$. To show that the pencil with carrier (d) is contained with multiplicity $(\lambda - \lambda_d)$ in the envelope, it is enough to prove that $(V-d)^{\lambda-\lambda_d}$ divides $f(U,V)$. (If (d) is a sharply $(q-\lambda)$-uniform direction then $S(d) \neq 0$ and this shows that $V-d$ cannot divide $f(U,V)$, so in this case the pencil with carrier (d) cannot be contained in the envelope.) To do this, we will show

$$(V-d)^{\lambda-\lambda_d} \mid S(V), S_1(V), S_2(V), \dots, S_\lambda(V).$$

For $1 \leq k \leq \lambda$ put $H(d)^{(k)}$ to denote the kth column of $H(d)$. For the integer k, $1 \leq k \leq \lambda - \lambda_d$ by (6) applied for the integers j where $\lambda - k - \lambda_d \leq j \leq 2\lambda - k - \lambda_d - 1$, in $H(d)$ we obtain that $H(d)^{(k)}$ is the linear combination of $H(d)^{(k+1)}, H(d)^{(k+2)}, \dots, H(d)^{(k+\lambda_d)}$. Hence the column space of $H(d)$ is generated by the last λ_d columns of $H(d)$, so the rank of this matrix is at most λ_d. By (7), the column $C(d)$ is the linear combination of the columns of $H(d)$ and hence when $H(d)$ has rank at most λ_d, then so is $H_i(d)$ for each i. Then for $s > \lambda_d$ the $s \times s$ minors of $H(d)$ have determinant zero. Using Lemma 2.3 of [14] it follows that d is a $(\lambda - \lambda_d)$-fold root of $\det H(d) = S(d)$ and of $\det H_i(d) = S_i(d)$ as we claimed.

If $\lambda_d = 0$ for some $(d) \in \mathcal{E}_\lambda$, then M_d contains the same number of copies of each element of $\mathbb{F}_q$ and hence $\pi_0(d) = \cdots = \pi_{2\lambda-2}(d) = 0$, so $H(d)$ is the $\lambda \times \lambda$ null-matrix. From Lemma 2.3 of [14], it follows that d is a λ-fold root of $\det H(d) = S(d)$ and of $\det H_i(d) = S_i(d)$, thus $(V - d)^\lambda$ divides $f(U, V)$. □

The next example shows the sharpness of Theorem 3.3.

Example 3.4. In AG$(2, q)$, q even, let U denote a subset consisting of λ points of a parabola. Assume that there are at least λ directions $(u_i) \neq (\infty)$ incident with λ 1-secants of U (this always happens if $\lambda(\lambda-1)/2 < q-\lambda$). For $(d) \in \ell_\infty \setminus \{(\infty)\}$ denote by N_d the number of 2-secants of U incident with (d). Then the directions of $\ell_\infty \setminus \{(\infty)\}$ are $(q-\lambda)$-uniform (with 0 modulo 2 as typical intersection number, and the renitent lines are the 1-secants of U). More precisely, the direction (d) is sharply $(q-\lambda_d)$-uniform, where $\lambda_d = \lambda - 2N_d$.

Then the product of the pencils centered at (d), for each (d) with $N_d > 0$, taking each of them with multiplicity $\lambda - \lambda_d = 2N_d$, is an envelope of class

$$2\sum_d N_d = \lambda(\lambda - 1).$$

Recall that there were at least λ sharply $(q-\lambda)$-uniform directions and so the points of U are incident with at least λ renitent lines with a sharply $(q-\lambda)$-uniform slope. Hence the renitent lines with a sharply $(q-\lambda)$-uniform direction cannot be covered by an envelope of class less than λ. But they can be covered by an envelope of class λ: the product of λ pencils centered at the points of U. In total we obtain an envelope of class $\lambda(\lambda-1)+\lambda = \lambda^2$ and there is no envelope with smaller class with the given properties.

Consider the envelope ensured by Theorem 3.3. The renitent lines incident with sharply $(q-\lambda)$-uniform directions of $\mathcal{E}_\lambda$ are contained in a factor of degree at least λ (since the sharply $(q-\lambda)$-uniform directions are incident with λ of these lines, and pencils centered at such directions are not contained in the envelope) and hence from the second part of the previous theorem the following is clear.

Corollary 3.5. *Suppose that the assumptions of the previous theorem holds. Then there are at most $\lambda^2 - \lambda$ directions incident with less than λ renitent lines. More precisely, if λ_d denotes the number of renitent lines with slope d for every $(d) \in \mathcal{E}_\lambda$, then*

$$\sum_{(d)\in\mathcal{E}_\lambda} (\lambda - \lambda_d) \leq \lambda^2 - \lambda.$$

It is also immediate that the number of renitent lines is at least $\lambda|\mathcal{E}_\lambda| - (\lambda^2 - \lambda) = \lambda(|\mathcal{E}_\lambda| + 1 - \lambda)$. □

4. The resultant method

The next result was developed in a series of papers by Szőnyi and Weiner [14,15], see also [13] and the Appendix of [16] for the version that we cite here.

Result 4.1 (*Szőnyi–Weiner Lemma*)**.** *Let $f, g \in \mathbb{F}[X, Y]$ be polynomials over the arbitrary field $\mathbb{F}$. Assume that the coefficient of $X^{\deg f}$ in f is not 0 and for $y \in \mathbb{F}$ put $k_y = \deg \gcd(f(X, y), g(X, y))$. Then for any $y_0 \in \mathbb{F}$*[2]

$$\sum_{y\in\mathbb{F}} (k_y - k_{y_0})^+ \leq (\deg f - k_{y_0})(\deg g - k_{y_0}). \tag{9}$$

[2] Here $\alpha^+ = \max\{0, \alpha\}$. Note that g can be the zero polynomial as well, in that case $\deg f = k_y = k_{y_0}$ and the lemma claims the trivial $0 \leq 0$.

The main ingredient of the next proofs is how we define the polynomials $f(X,Y)$ and $g(X,Y)$ in the above lemma. In order to be able to detect the renitent lines at the $(q-\lambda)$-uniform directions, in the definition of g we introduce an auxiliary polynomial h that we obtain by interpolation.

This method does not reveal the underlying envelope, but it can be used to deduce quantitative information about the reintent lines. First we show an alternative proof of Corollary 3.5. Note that in this proof we do not need the $\lambda \le (q-1)/2$ condition which was used in Theorem 3.3 to construct the envelope. Then we will show another quantitative result: we prove that each affine point is incident either with just a "few" or with a "lot" of renitent lines.

Second proof of Corollary 3.5. Put $|\mathcal{E}_\lambda| = k$, $\mathcal{E}_\lambda = \{(1 : d_i : 0)\}_{i=1}^k$ and $\mathcal{T} = \{(a_i : b_i : 1)\}_{i=1}^{|\mathcal{T}|}$. Denote by m_i the typical intersection number corresponding to the point $(1 : d_i : 0)$. We will need the polynomial $h(Y) := \sum_{i=1}^k m_i(1-(Y-d_i)^{q-1}) \in \mathbb{F}_q[Y]$. Then $h(d_i) \equiv m_i \pmod p$ for each $1 \le i \le k$. Next define the polynomials

$$f(X,Y) := X^q - X,$$

$$g(X,Y) := \sum_i (X + a_iY - b_i)^{q-1} - |\mathcal{T}| + h(Y).$$

Note that g encodes the intersection numbers of the lines $[d : -1 : x]$ with $\mathcal{T}$, i.e. $g(x,d) \equiv h(d) - |[d:-1:x] \cap \mathcal{T}| \pmod p$. For a direction $(y) \in \mathcal{E}_\lambda$ let λ_y denote the number of renitent lines incident with (y). Then for any $(y) \in \mathcal{E}_\lambda$ it holds that

$$k_y := \deg \gcd(f(X,y), g(X,y)) = q - \lambda_y.$$

Then for any fixed $(r) \in \mathcal{E}_\lambda$, (9) gives

$$\sum_{(y)\in\mathcal{E}_\lambda} (\lambda_r - \lambda_y) \le \sum_{y\in\mathbb{F}_q} (\lambda_r - \lambda_y)^+ \le \lambda_r(\lambda_r - 1).$$

If we choose (r) so that $\lambda_r = \lambda$, then

$$k\lambda - \sum_{(y)\in\mathcal{E}_\lambda} \lambda_y \le \lambda(\lambda-1)$$

and hence

$$\sum_{(y)\in\mathcal{E}_\lambda} (\lambda - \lambda_y) \le \lambda^2 - \lambda \quad \text{and} \quad \lambda(k+1-\lambda) \le \sum_{(y)\in\mathcal{E}_\lambda} \lambda_y. \quad \square$$

Theorem 4.2. *Take a multiset $\mathcal{T}$ of $\mathrm{AG}(2,q)$, $q > 2$, and fix an integer $\lambda > 0$. Let $\mathcal{F}_\lambda$ denote the set of $(q-\lambda)$-uniform directions. If $|\mathcal{F}_\lambda| > \lambda^2 + \lambda$ then for each point R of the plane it holds that R is incident with at most λ or with at least $|\mathcal{F}_\lambda| + 1 - \lambda$ renitent lines.*

Proof. First we prove the following. If $\mathcal{E}_\lambda$ is a set of at most q directions which are $(q-\lambda)$-uniform and $|\mathcal{E}_\lambda| > \lambda^2 + \lambda$, then for each point R of the plane it holds that R is incident with at most λ or with at least $|\mathcal{E}_\lambda| + 1 - \lambda$ renitent lines with slope in $\mathcal{E}_\lambda$.

Consider $\mathrm{AG}(2,q)$ embedded in $\mathrm{PG}(2,q)$ as $\{(a : b : 1) : a, b \in \mathrm{GF}(q)\}$ and apply a collineation of $\mathrm{PG}(2,q)$ which maps the line $[0:0:1]$ (the line at infinity) to the line $[1:0:0]$ (the Y-axis) such that $(0:1:0)$ is not in the image of $\mathcal{E}_\lambda$. It may be further assumed that this collineation maps R to some point $(1 : y_0 : 0)$. Denote the image of $\mathcal{T}$ by $\{(a_i : b_i : 1)\}_i \cup \{(1 : z_j : 0)\}_j$ and the image of $\mathcal{E}_\lambda$ by $\{(0 : c_k : 1)\}_k$.

Let m_k be the typical intersection number corresponding to the point $(0 : c_k : 1)$. We will need the polynomial $h(X) = \sum_{k=1}^{|\mathcal{E}_\lambda|} m_k(1-(X-c_k)^{q-1}) \in \mathbb{F}_q[X]$. Then $h(c_k) \equiv m_k \pmod p$ for each

$k \in \{1, \dots, |\mathcal{E}_\lambda|\}$. Next define the polynomials

$$f(X,Y) := \prod_{k=1}^{|\mathcal{E}_\lambda|}(X - c_k),$$
$$g(X,Y) := \sum_i (X + a_i Y - b_i)^{q-1} + \sum_j (Y - z_j)^{q-1} - |\mathcal{T}| + h(X).$$

As before, g encodes the intersection multiplicities of the lines $[d : -1 : x]$ with $\mathcal{T}$, i.e. $g(x,d) \equiv h(d) - |[d : -1 : x] \cap \mathcal{T}| \pmod p$. For a point $P \in \mathrm{PG}(2,q)$ let $\operatorname{ind} P$ denote the number of renitent lines incident with P. Then for any $y \in \mathbb{F}_q$ it holds that

$$k_y := \deg \gcd(f(X,y), g(X,y)) = |\mathcal{E}_\lambda| - \operatorname{ind}(1 : y : 0).$$

Then (9) gives

$$\sum_{y \in \mathbb{F}_q} (\operatorname{ind} R - \operatorname{ind}(1 : y : 0))^+ \le \operatorname{ind} R(q - 1 - |\mathcal{E}_\lambda| + \operatorname{ind} R).$$

Note that

$$\sum_{y \in \mathbb{F}_q} \operatorname{ind}(1 : y : 0) \le |\mathcal{E}_\lambda|\lambda$$

and hence

$$q \operatorname{ind} R - |\mathcal{E}_\lambda|\lambda \le \operatorname{ind} R(q - 1 - |\mathcal{E}_\lambda| + \operatorname{ind} R),$$

$$0 \le (\operatorname{ind} R)^2 - \operatorname{ind} R(|\mathcal{E}_\lambda| + 1) + |\mathcal{E}_\lambda|\lambda.$$

For $\operatorname{ind} R = \lambda + 1$, or $\operatorname{ind} R = |\mathcal{E}_\lambda| - \lambda$ we have

$$(\operatorname{ind} R)^2 - \operatorname{ind} R(|\mathcal{E}_\lambda| + 1) + |\mathcal{E}_\lambda|\lambda = \lambda^2 + \lambda - |\mathcal{E}_\lambda|,$$

which is less than 0 since $|\mathcal{E}_\lambda| > \lambda^2 + \lambda$. This proves $\operatorname{ind} R \le \lambda$ or $\operatorname{ind} R \ge |\mathcal{E}_\lambda| - \lambda + 1$.

Of course, if $|\mathcal{F}_\lambda| \le q$ then one can take $\mathcal{E}_\lambda = \mathcal{F}_\lambda$ and this proves the theorem.

Now assume $q+1 = |\mathcal{F}_\lambda| > \lambda^2+\lambda$ and take an affine point R. We have to show that R is incident with at most λ or with at least $q+2-\lambda$ renitent lines. Define $\mathcal{E}_\lambda$ as any subset of directions of size q. Note that $q+1 = |\mathcal{F}_\lambda| \ne \lambda^2+\lambda+1$ because this would imply $q = \lambda(\lambda+1)$ and hence $\lambda = 1$ and $q = 2$, which we excluded. It follows that $|\mathcal{E}_\lambda| = q > \lambda^2+\lambda$ and hence the arguments above show that R is incident with at most $\lambda+1$ renitent lines or with at least $q+1-\lambda$ renitent lines. We have to exclude the cases when R is incident with exactly $\lambda+1$ renitent lines or with exactly $q+1-\lambda$ renitent lines.

If the former case holds, then take a direction S such that RS is not renitent and define $\mathcal{E}_\lambda$ as $\ell_\infty \setminus \{S\}$. Then the renitent lines incident with R have slopes in $\mathcal{E}_\lambda$, a contradiction since there are more than λ but less than $q+1-\lambda$ of them.

If the latter case holds, then take a direction S such that RS is renitent and, as before, define $\mathcal{E}_\lambda$ as $\ell_\infty \setminus \{S\}$. Then there are exactly $q-\lambda$ renitent lines incident with R with slopes in $\mathcal{E}_\lambda$, a contradiction since this number should be at least $q+1-\lambda$ or at most λ (recall that $q+1 = |\mathcal{F}_\lambda| > \lambda^2+\lambda$). □

With some further efforts, the earlier methods by Szőnyi and Weiner [14,15], see also [13,17], also provide an alternative, but more laborious, route to reach similar results as in Section 3.

5. The dual statements and codewords of PG(2, q) the dual statements and codewords of PG(2,q)

In this section, we will dualize some of the earlier theorems and we will show how they apply for codewords of $\mathrm{PG}(2,q)$. The dual version of Theorem 2.1 (allowing also $|\mathcal{E}| = q+1$ and not only $|\mathcal{E}| \le q$, as a consequence of Theorem 2.4, see Remark 2.5) is the following.

Theorem 5.1. *Fix a point Q of $\mathrm{PG}(2,q)$. Take a multiset of lines $\mathcal{L}$ in $\mathrm{PG}(2,q)$, none of them containing Q. Let $\mathcal{E}_\lambda$ denote a non-empty set of lines through Q. Assume that*

(i) $0 < \lambda \le \min\{q-2, p-1\}$,
(ii) *for each line $z \in \mathcal{E}_\lambda$, there are at most λ points which are incident with t_z modulo p lines of $\mathcal{L}$ (counted with multiplicities); we call these points renitent,*
(iii) *for each $z \in \mathcal{E}_\lambda$ the remaining points of $z \setminus \{Q\}$ are incident with m_z (the typical covering number of z) modulo p lines of $\mathcal{L}$, and the values $t_z - m_z$ modulo p do not depend on the choice of z.*

Then the renitent points incident with lines of $\mathcal{E}_\lambda$ are contained in an algebraic curve of degree λ.

Note that one may formulate the dual version of Theorems 2.4 and 3.3 similarly.

Definition 5.2. Let $C_1(2,q)$ be the p-ary linear code generated by the incidence vectors of the lines of $\mathrm{PG}(2,q)$, $q = p^h$, p prime.

The next result proves a nice geometric property on codewords of $\mathrm{PG}(2,q)$.

Result 5.3 (*Blokhuis, Brouwer, Wilbrink [10, Proposition, p. 66]*)**.** *Let X be a subset of $\mathrm{PG}(2,q)$ whose characteristic vector is a codeword of $C_1(2,q)$ and let Q be a point not in X. Then the points P for which the line QP is tangent to X (i.e., $QP \cap X = \{P\}$) are all collinear.*

The next theorem follows easily from Theorem 5.1 and it is the generalization of Result 5.3.

Theorem 5.4. *Let X be a subset of $\mathrm{PG}(2,q)$ whose characteristic vector is a codeword c of $C_1(2,q)$ and let Q be a point in $\mathrm{PG}(2,q)$. Let $\mathcal{E}_\lambda$ denote a non-empty set of lines through Q, each of them incident with at most $\lambda \le \min\{q-2, p-1\}$ points of $X \setminus \{Q\}$. Then the points of $X \setminus \{Q\}$ incident with lines of $\mathcal{E}_\lambda$ are on a curve of degree λ.*

Proof. Put $\mathcal{E}_\lambda = \{z_1, \dots, z_{|\mathcal{E}_\lambda|}\}$. By definition, c is the linear combination of some lines e_j of $\mathrm{PG}(2,q)$, i.e. $c = \sum_j c_j e_j$, $c_j \in \mathbb{F}_p^*$. We define a multiset $\mathcal{L}$ of lines of $\mathrm{PG}(2,q)$ in the following way: if e_j is not incident with Q then the weight of e_j is c_j, all other lines have weight 0. On each line z_i there will be at most λ points of $X \setminus \{Q\}$ incident with t_{z_i} modulo p lines of $\mathcal{L}$ (counted with multiplicities) and the rest of the points will be incident with $m_{z_i} := (t_{z_i} - 1)$ modulo p lines of $\mathcal{L}$. Here $t_{z_i} = 1$ and $m_{z_i} = 0$ if z_i is not one of the e_js and $t_{z_i} = 1 - c_j$, $m_{z_i} = -c_j$ if $z_i = e_j$ for some j. Hence the result follows from Theorem 5.1. □

Note that from the theorem above, it follows that the assumption $\lambda \le p-1$ in Theorem 5.1 and so in Theorems 2.1 and 2.4 is sharp at least in case $q = p^2$. Blokhuis, Brouwer and Wilbrink [10] showed that the characteristic vector of a Hermitian unital in $\mathrm{PG}(2,q)$ is a codeword in $C_1(2,q)$. Let $\mathcal{H}$ be a Hermitian unital in $\mathrm{PG}(2,p^2)$ and let Q be a point of $\mathcal{H}$, $\mathcal{E}_\lambda$ be the set of p^2 lines through Q intersecting the unital in $p+1$ points. If Theorem 5.4 was true with $\lambda = p$, then it would yield that the points of $\mathcal{H} \setminus \{Q\}$ are on a curve $\mathcal{C}$ of degree p. But through any point of $\mathcal{H} \setminus \{Q\}$, there pass $p^2 - 1$ lines intersecting $\mathcal{H} \setminus \{Q\}$ in $p+1$ points. Hence by Bézout's theorem these lines would be linear factors of the curve $\mathcal{C}$; which is a contradiction since the degree of $\mathcal{C}$ is $p < p^2 - 1$.

Acknowledgment

The authors are grateful to the anonymous referees for their valuable comments and suggestions which have certainly improved the quality of the manuscript.

References

[1] M. Simonovits, Some of my favorite Erdős theorems and related results, theories, in: G. Halász, L. Lovász, M. Simonovits, V.T. Sós (Eds.), Paul ErdőS and His Mathematics, Vol. II, Springer, 2002, pp. 565–635.
[2] A.J.W. Hilton, E.C. Milner, Some intersection theorems for systems of finite sets, Quart. J. Math. Oxford Ser. 18 (2) (1967) 369–384.

[3] S. Ball, M. Lavrauw, Arcs in finite projective spaces, EMS Surv. Math. Sci. 6 (2019) 133–172.
[4] T. Szőnyi, Zs. Weiner, Stability of k mod p multisets and small weight codewords of the code generated by the lines of PG$(2, q)$, J. Combin. Theory Ser. A 157 (2018) 321–333.
[5] B. Csajbók, Zs. Weiner, Generalizing Korchmáros–Mazzocca arcs, Combinatorica 41 (2021) 601–623.
[6] A. Blokhuis, T. Szőnyi, Note on the structure of semiovals, Discrete Math. 106/107 (1992) 61–65.
[7] A. Blokhuis, Characterization of seminuclear sets in a finite projective plane, J. Geom. 40 (1991) 15–19.
[8] T. Szőnyi, On the number of directions determined by a set of points in an affine Galois plane, J. Combin. Theory Ser. A 74 (1996) 141–146.
[9] S. Ball, Polynomials in finite geometries, in: J.D. Lamb, et al. (Eds.), Surveys in Combinatorics, 1999, in: Lond. Math. Soc. Lect. Note Ser., vol. 267, Cambridge University Press, 1999, pp. 17–35.
[10] A. Blokhuis, A.E. Brouwer, H. Wilbrink, Hermitian unitals are code words, Discrete Math. 97 (1991) 63–68.
[11] P. Sziklai, On subsets of GF(q^2) with dth power differences, Discrete Math. 208/209 (1999) 547–555.
[12] A. Seidenberg, Elements of the Theory of Algebraic Curves, Addison–Wesley, Reading, Mass, 1968.
[13] P. Sziklai, Polynomials in Finite Geometry, Manuscript available online at https://www.academia.edu/69422637/Polynomials_in_finite_geometry.
[14] Zs. Weiner, On (k, p^e)-arcs in Desarguesian planes, Finite Fields Appl. 10 (2004) 390–404.
[15] T. Szőnyi, On the embedding of (k, p)-arcs in maximal arcs, designs, Codes Cryptogr. 18 (1999) 235–246.
[16] T. Héger, Some Graph Theoretic Aspects of Finite Geometries (Ph.D. thesis), Eötvös Loránd University, 2013, http://heger.web.elte.hu//publ/HTdiss-e.pdf.
[17] A. Blokhuis, T. Szőnyi, Zs. Weiner, On sets without tangents in Galois planes of even order, designs, Codes Cryptogr. 29 (2003) 91–98.