Note

On the Number of Directions Determined by a Set of Points in an Affine Galois Plane

TAMÁS SZÖNYI

Department of Computer Science, Eötvös Loránd University, Budapest, H-1088, Budapest, Múzeum krt. 6-8, Hungary

Communicated by J. H. van Lint

Received May 10, 1994; revised November 23, 1994

In this paper the number of directions determined by a set of \( q - n \) points of \( AG(2, q) \) is studied. To such a set we associate a curve of degree \( n \) and show that its linear components correspond to points that can be added to the set without changing the set of determined directions. The existence of linear components is guaranteed by Weil's theorem concerning the number of \( GF(q) \)-rational points of an absolutely irreducible curve, if \( n \) is small enough.

In this note we shall work on the affine and projective plane over the finite field \( GF(q) \) of \( q \) elements, denoted by \( AG(2, q) \) and \( PG(2, q) \), respectively. Here \( q \) is a prime-power, \( q = p^h \) (\( p \) is a prime, \( h > 0 \) is an integer). We use cartesian coordinates in \( AG(2, q) \), usually denoted as \((x, y)\). Infinite points can be identified with directions. The infinite point \((m)\) corresponds to the parallel class of lines with equation \( mx + b = 0 \). The direction \( m \) is also called the slope of such a line.

In his book [6] Rédei developed the theory of fully reducible lacunary polynomials over finite fields. His results are not only interesting in themselves, but they have several interesting and highly non-trivial applications in number theory and algebra. For recent developments motivated by Rédei's theory, see Blokhuis [2]. One of the applications [6, Section 36] is the following: given a set \( U \) of \( q \) points in \( AG(2, q) \) what can the number of directions determined by \( U \) be? Here we say that the direction \( (m) \) is determined by \( U \) if there is a line \( mx + b - y = 0 \) spanned by two points of \( U \). The results of Rédei give very strong bounds on the number \( N \) of directions determined by a point set consisting of \( q \) points.

In the particular case \( q = p \) prime, Lovász and Schrijver [5] proved \( N \geq (p + 3)/2 \) without using Rédei's theory. They also showed that a set...
determining \((p + 3)/2\) directions can be written as \(\{(x, x^{(p + 1)/2}); x \in \text{GF}(p)\}\) in a suitable coordinate system. The bound \(N \geq (p + 3)/2\) was also obtained by Rédei and Meyges in [6, Section 36].

The general case is more complicated. For a survey of the results, including a recent improvement by Blokhuis, Brouwer, and Szőnyi, the reader is referred to [2, 3].

The aim of this paper is to study the number of directions determined by a set of less than \(q\) points. Our main result (Theorem 4) shows that a set \(U\) with \(|U| < q - \sqrt{q}/2\) either determines at least \((q + 1)/2\) directions or is contained in a set \(V\) with \(|V| = q\), and \(V\) determines precisely the directions determined by \(U\). For \(q = p\) a prime, the term \(\sqrt{q}/2\) is improved in the remarks following Theorem 4.

**Definition 1.** Let \(D\) be a set of directions. We say that a subset \(U\) of \(\text{AG}(2, q)\) is a \(D\)-set if \(U\) determines precisely the directions belonging to \(D\). A \(D\)-set is said to be complete if it is maximal subject to set theoretical inclusion.

In other words, a \(D\)-set \(U\) is complete if for every \(u \in U\) the set \(U \setminus \{u\}\) determines a direction not belonging to \(D\). For a \(D\)-set \(U\) we have \(|U| \geq q\), since \(|U| > q\) implies that at least one line from every parallel class contains more than one point of \(U\).

**Proposition 2.** Let \(\mathcal{C}_n (n \geq 2)\) be a curve of order \(n\) defined over \(\text{GF}(q)\) and denote by \(N\) the number of points of \(\mathcal{C}_n\) in \(\text{PG}(2, q)\). Moreover, suppose that \(\mathcal{C}_n\) does not contain a linear component defined over \(\text{GF}(q)\), and \(n - q/2\).

\(1)\) \(N \leq n(q + 1)/2\), moreover,

\(2)\) \(N = n(q + 1)/2\) implies that \(\mathcal{C}_n\) is the union of conics (hence, \(n\) is even).

**Proof.** Suppose first that \(\mathcal{C}_n\) is absolutely irreducible. Weil's theorem (see [4, p. 228]) gives that \(N \leq q + 1 + (n - 1)(n - 2)/2\). This can be obtained as the union of irreducible components: \(\mathcal{C}_n = \mathcal{D}_1 \cup \cdots \cup \mathcal{D}_{j_1}\). Here the indices \(j_i\) denote the order of the component, hence, \(n = \sum_{i=1}^{j_1} j_i\). If \(\mathcal{D}_{i_0}\) is defined over \(\text{GF}(q)\) and \(N_{i_0}\) denotes the number of its points in \(\text{PG}(2, q)\) then the first part of the proof shows that \(N_{i_0} \leq j_{i_0}(q + 1)/2\). If \(\mathcal{D}_{i_0}\) cannot be defined over \(\text{GF}(q)\), then it is easy to see that \(N_{i_0} \leq j_{i_0}^2\) (see, e.g., Lemma 10.1.1. of [4]). Hence, we have in this case that \(N_{i_0} \leq j_{i_0}(q + 1)/2\). Finally, since \(N \leq \sum_{i=1}^{j_1} j_i = n(q + 1)/2\), the assertion of (1) follows. Since for absolutely irreducible curves it was shown that equality was possible only for curves of order 2, (2) follows as well.
Remark 3. Instead of Weil’s theorem we could use other bounds on the number \( N \) of \( GF(q) \)-rational points of a curve. For example, in the case \( q = p \) a prime, the Stöhr–Voloch bound (see [8, lemma]) saying that \( N \leq 2n(n - 3) + 2n(p + 5)/5 \) yields that \( n < (p + 45)/20 \) is enough (instead of \( n \leq \sqrt{q}/2 \)) to deduce the same conclusion as in Proposition 3.

Notation. Let \( A \) be a \((m)\)set of elements of \( GF(q) \). The \( k \)-th elementary symmetric polynomial of these elements will be denoted by \( \sigma_k(A) \).

Theorem 4. Let \( U \) be a \((m)\)set of \( AG(2, q) \) consisting of \( q - n \) points, \( n \leq \sqrt{q}/2 \). Moreover, suppose that \( |D| < (q + 1)/2 \). Then \( U \) is incomplete; that is, it can be extended to a \((m)\)set \( Y \) with \( |Y| = q \).

Proof. Let \( U = \{ (a_i, b_i) ; i = 1, ..., q - n \} \) be our \((m)\)set of \( q - n \) points of \( AG(2, q) \). We can suppose that \((\infty) \in D\) and define the polynomial

\[ H(x, y) = \prod_{i=1}^{q-n} (x + ya_i - b_i) = \sum_{j=0}^{q-n} h_j(y)x^{q-n-j}. \]

Note that \( \deg(h_j) \leq j \). Let \( H_j(x) = H(x, y) \). Then \( H_j(x) \) is a divisor of \( x^n - x \) if and only if the elements \(-a_iy + b_i ; i = 1, ..., q - n\) are pair-wise distinct, that is, when \((y) \notin D\). In this case we can find out what \((x^n - x)/H_j(x)\) is. Knowing the elementary symmetric polynomials of the subset \( A_j = \{ -a_iy + b_i ; i = 1, ..., q - n \} \), the elementary symmetric polynomials of the remaining elements (denoted by \( \sigma(GF(q) \backslash A_j) \)) can be computed using the coefficients of \( H_j(x) \). For example,

\[ \sigma^*_j := \sigma_j(GF(q) \backslash A_j) = -\sigma_j(A_j) + h_j(y), \]

\[ \sigma^*_k := \sigma_k(GF(q) \backslash A_j) = -\sigma_k(A_j) - \sigma_j(GF(q) \backslash A_j)\sigma_j(A_j) = -h_k(y) + (h_j(y))^2, \]

and one can continue recursively:

\[ \sigma^*_j := \sigma_j(GF(q) \backslash A_j) = -\sigma_j(A_j) - \sum_{k=1}^{j-1} \sigma_k(A_j)\sigma_{j-k}(GF(q) \backslash A_j). \]

Since \( \sigma_j(A_j) = (-1)^j h_j(y) \) and \( h_j(y) \) has degree at most \( j \), it is easy to see by induction that \( \sigma^*_j \) has degree at most \( j \). Now define the polynomial \( f(x, y) = x^n - \sigma_1(GF(q) \backslash A_j)x^{n-1} + \sigma_2(GF(q) \backslash A_j)x^{n-2} - \cdots + (-1)^{n} \sigma_n(GF(q) \backslash A_j) \).

First of all, note that \( f \) of total degree \( n \) and \( H(x, y)/f(x, y) = x^n - x \) if \((y) \notin D\). For \((y_0) \notin D\), the polynomial \( f(x, y_0) \) is just the product \( \prod_{a_i \in GF(q) \backslash A_{y_0}} (x - a_i) \); hence for \((y_0) \notin D\), the curve \( \mathcal{F} \) defined by
\( f(x, y) = 0 \) has precisely \( n \) distinct points \((x, y_0)\). Since the degree of \( f \) is \( n \), these points are necessarily simple. Therefore \( \mathcal{F} \) has at least
\[ N = (q + 1 - |D|)n \] (simple) points in \( \text{PG}(2, q) \). If \( |D| < (q + 1)/2 \), then \( N > n(q + 1)/2 \); hence Proposition 3 yields that \( \mathcal{F} \) must contain a linear component defined over \( \text{GF}(q) \). Since \( f \) contains the term \( x^n \), the equation of this linear component can be written in the form \( x + ay - b \) for some \( a, b \in \text{GF}(q) \). This implies that \(-ay + b \notin A_f \) for all \((y) \notin D \). If we consider \( U^* = U \cup \{(a, b)\} \) and write the corresponding polynomial \( H^*(x, y) = H(x, y)(x + ay - b) \), then \( H^*(y, x) \) divides \( x^q - x \) for \((y) \notin D \), since \( H(x, y)f(x, y) = x^q - x \) and \( x + ay - b \) divides \( f(x, y) \). But this divisibility means that \( U^* \) does not determine the directions \((y) \notin D \); hence \( U^* \) is also a \( D \)-set. By repeating this procedure we end up with a \( D \)-set \( Y \) consisting of \( q \) points.

The above proof shows that the bound \( n \leq \sqrt{q}/2 \) can be improved if \( |D| \) is essentially smaller than \((q + 1)/2 \). As in Remark 3, the Stöhr–Voloch bound (see [8, lemma]) shows that in the case \( q = p \) prime, \( n < (p + 45)/20 \) is enough to deduce the same conclusion as in Theorem 4.

Remark 5. For the sake of simplicity, suppose that \( q = p \) is prime. A (simple) bound (see Stöhr–Voloch [7, Theorem 0.1]) says that an absolutely irreducible curve of degree \( d \) has at most \( d(q + d - 1)/2 \) points if it has a simple point which is not an inflexion. This last condition is automatically satisfied if \( d < p \). Using this in the proof of Theorem 4, one can conclude that a \( D \)-set with \([U] = p - n \) is incomplete when \( |D| < (p + 3 - n)/2 \). In other words, a set of \( p - n \) points determine at least \((q + 3 - n)/2 \) directions if \( q = p \) is prime. We just remark without the details that exactly the same result can be proved using lacunary polynomials (cf. [2, Theorem 5; 3, Proposition 2 \((e = 0)\); 6, pp. 34–35]).

Remark 6. There is a nice similarity between the theory of complete arcs, and our theorem. Definition 1 and the formulation of the theorems try to stress on this similarity. In case of arcs, Bose’s theorem says that the maximum number of points that an arc can have is \( q + 1 \) or \( q + 2 \), according as \( q \) is odd or even. Segre’s famous theorem shows that if an arc has cardinality which is close to this (more precisely, larger than \( q - \sqrt{q} + 1 \), if \( q \) is even; \( q - \sqrt{q}/2 + 7/4 \), if \( q \) is odd), then it is always contained in an arc having maximum cardinality. (We just mentioned the original bound by Segre; there are recent improvements on it (see e.g., Voloch, [8]).) For Segre’s proof and other results the reader is referred to the book [4, Chaps. 9, 10]. Actually, our method is similar to Segre’s one, also, in the sense that an algebraic curve is associated to the set and bounds on the number of \( \text{GF}(q) \)-rational points of a curve (like Weil’s theorem, Stöhr–Voloch bound) are needed.
Remark 7. In the particular case $n = 1$ the above proof is very short; the polynomial $(x^q - x)/H, x)$ is just $x - \sum a_i y + \sum b_i$. In other words, this means that the point $A = (\sum a_i, -\sum b_i)$ can be added without changing the set of directions determined by the point set. Note that for each direction $(y) \notin D$ there is precisely one line $L_y$ disjoint to $U$ and we just showed that these lines pass through A. Segre's "Lemma of tangents" (see [4, Chap. 10]) is similar to this observation. The proof can also be regarded as a new proof of Proposition 2 in Blokhuis [1].

Let us mention a very interesting open problem: it would be desirable to improve the bound on $D$ by one, that is, to show a similar embedding theorem also for $|D| = (q + 1)/2$. It is worth pointing out that such an improvement really needs a bound on $n$ compared to $q$ as the following simple example shows: Take $q = 7$ and consider a parallelogram in $AG(2, q)$. This parallelogram, together with its center, forms a set of five points determining exactly four directions (the sides and the diagonals of the parallelogram). Hence, in our case $q = 7, n = 2$, and $|D| = 4 = (q + 1)/2$. When $|D| = (q + 1)/2$ the next proposition shows that $D$ is projectively unique.

Proposition 6. Let $U$ be a complete $D$-set, $|D| = (q + 1)/2$, $|U| = q - n \geq q - \sqrt{q}/2$. Then $GF(q) \setminus D$ is the projection of an irreducible conic from the infinite point $(0)$ of the $x$-axis onto the $y$-axis, and the point is internal with respect to the conic.

Proof. If $|D| = (q + 1)/2$, then the curve $F$ introduced in the proof of Theorem 4 must be the union of conics and $F$ cannot have other points than the points belonging to $(y) \notin D$. Let $C$ denote such a component. Since $|D| = (q + 1)/2$, $GF(q) \setminus D$ is just the set of all $y$'s for which $F$ (and hence $C$) has $GF(q)$-rational points; hence it is indeed the projection of $C$ onto the $y$-axis. In the proof of Theorem 4 we saw that for all these $y$'s there are precisely $n$ points of $F$; hence $C$ has precisely two points on each of these lines. Therefore $C$ cannot have tangents passing through $(0)$; i.e., $(0)$ is internal with respect to $C$.

Acknowledgment

The research was supported by Hungarian National Science Foundation (OTKA) Grants T-014105 and T-014302.

References