ON THE GRAPH OF A FUNCTION IN MANY VARIABLES OVER A FINITE FIELD

SIMEON BALL

ABSTRACT. Some improved bounds on the number of directions not determined by a point set in the affine space $\mathrm{AG}(k,q)$ are presented. More precisely, if there are more than $p^e(q-1)$ directions not determined by a set of q^{k-1} points $\mathcal{S}$ then every hyperplane meets $\mathcal{S}$ in 0 modulo p^{e+1} points. This bound is shown to be tight in the case $p^e = q^s$ and when $q = p^{es}$ sets of q^{k-1} points that do not meet every hyperplane in 0 modulo p^{e+1} points and have a little less than $p^e(q-1)$ non-determined directions are constructed.

1. Introduction

Let $\mathrm{AG}(k,q)$ denote the k-dimensional affine space over $\mathrm{GF}(q)$. For any two points x and y of $\mathrm{AG}(k,q)$ the *direction determined by* x *and* y is the projective point d of $\mathrm{PG}(k-1,q)$, where $d = \langle (x-y) \rangle = \{\lambda(x-y) \mid \lambda \in \mathrm{GF}(q)\}$. For every $d \in \mathrm{PG}(k-1,q)$ there are q^{k-1} parallel affine lines with direction d, so every set of more than q^{k-1} affine points determines every direction by the pigeon-hole principle.

The following theorem deals with the case when a set of q^{k-1} points does not determine many directions. The case $k=2$ is proved in [5] (for a simpler proof and for small characteristics see [1]) and the case $k \geq 3$ is proved in [6].

THEOREM 1.1. *If there are more than $(q^{k-1}-q^{k-2})/2$ directions not determined by a set $\mathcal{S}$ of q^{k-1} points in $AG(k,q)$ then $\mathcal{S}$ is a $GF(q_0)$-linear set for some subfield $GF(q_0)$ of $GF(q)$.*

Note that if q is prime then the previous theorem implies that $\mathcal{S}$ is simply a subspace of dimension $k-1$. It also implies, in general, that if a line is incident with more than one point of $\mathcal{S}$ then it is incident with 0 modulo q_0 points of $\mathcal{S}$.

In [4] (for the case $k=3$) and [3] it was shown that even when the hypothesis on the number of directions not determined by the set of points is significantly reduced some extra properties of $\mathcal{S}$ remain.

THEOREM 1.2. *Let $q = p^h$ and $1 \leq p^e < q^{k-2}$, where $e \in \mathbb{Z}$. If there are at least $p^e q$ directions not determined by a set $\mathcal{S}$ of q^{k-1} points in $AG(k,q)$ then every hyperplane meets $\mathcal{S}$ in 0 modulo p^{e+1} points.*

In this article the following improvement to the previous theorem is given with a shorter and simpler proof. The main difference here is the use of $\mathrm{GF}(q) \times \mathrm{GF}(q^{k-1})$ as a model for $\mathrm{AG}(k,q)$ in place of the natural $\mathrm{GF}(q)^k$.

Date: 4 September 2006.
The author acknowledges the support of the Ministerio de Ciencia y Tecnologia, España.

THEOREM 1.3. *Let $q = p^h$ and $1 \leq p^e < q^{k-2}$, where $e \in \mathbb{Z}$. If there are more than $p^e(q-1)$ directions not determined by a set $\mathcal{S}$ of q^{k-1} points in $AG(k,q)$ then every hyperplane meets $\mathcal{S}$ in 0 modulo p^{e+1} points.*

In Section 3 sets of points that reach the bound in the case $p^e = q^s$ and almost reach the bound when $q = p^{es}$ are constructed.

If f is a function in $k-1$ variables over the finite field $\mathrm{GF}(q)$ then the set of points $\mathcal{S} = \{(x, f(x)) \mid x \in \mathrm{GF}(q)^{k-1}\}$ is a set of q^{k-1} points of $\mathrm{AG}(k,q)$ and the set of directions determined by the function f is defined to be the set of directions determined by $\mathcal{S}$. We call $\mathcal{S}$ the *graph* of f, for obvious reasons. Note that for any set $\mathcal{S}$ of q^{k-1} points which does not determine all the directions, by applying an affine transformation so that the projective point $\langle(0,1)\rangle$ is a non-determined direction, we can construct a function whose graph is the set $\mathcal{S}$.

2. PROOF OF THEOREM 1.3

Proof. Let us consider the points of $\mathrm{AG}(k,q)$ as a set of elements of $\mathrm{GF}(q)\times\mathrm{GF}(q^{k-1})$ and $\mathcal{S}$ a set of q^{k-1} points. We can assume, after making an affine transformation if necessary, that the hyperplane with first coordinate zero does not contain exactly q^{k-2} points of $\mathcal{S}$. Then the set of directions not determined by $\mathcal{S}$ consists of projective points $\langle(1,m)\rangle$ where m runs through some set $\mathcal{N}$.

Let $x = (x_1, x_2)$ and $y = (y_1, y_2)$ be two points of $\mathrm{AG}(k,q)$ with the property that $x_1 \neq y_1$ and there is an element $n \in \mathrm{GF}(q^{k-1})$ such that $x_1 n - x_2 = y_1 n - y_2$. Then, $(x_1 - y_1)n = x_2 - y_2$ and the projective point $\langle(x_1-y_1, x_2-y_2)\rangle = \langle(1,n)\rangle$. Thus, $\langle(1,n)\rangle$ is the direction determined by the points x and y.

For all $m \in \mathcal{N}$ the projective point $\langle(1,n)\rangle$ is not determined by $\mathcal{S}$ and so the set

$$\{x_1 m - x_2 \mid x = (x_1, x_2) \in \mathcal{S}\}$$

consists of distinct elements, and hence all elements, of $\mathrm{GF}(q^{k-1})$.

Define a polynomial r in two variables and polynomials σ_j, in one variable of degree at most $j(q-1)$, by

$$r(X,Y) = \prod_{x\in\mathcal{S}}(X - (x_1 Y - x_2)^{q-1}) = \sum_{j=0}^{q^{k-1}} \sigma_j(Y) X^{q^{k-1}-j}.$$

Now r has the property that for all $m \in \mathcal{N}$,

$$r(X,m) = \prod_{x\in\mathcal{S}}(X - (x_1 m - x_2)^{q-1}) = \prod_{\lambda\in\mathrm{GF}(q^{k-1})}(X - \lambda^{q-1})$$

$$= X(X^{(q^{k-1}-1)/(q-1)} - 1)^{q-1} = X^{q^{k-1}} + X^{q^{k-1}-(q^{k-1}-1)/(q-1)} + \ldots + X.$$

Thus, for all $m \in \mathcal{N}$ and $1 \leq j < (q^{k-1}-1)/(q-1)$ we have $\sigma_j(m) = 0$. However, $|\mathcal{N}| > p^e(q-1) \geq \deg(\sigma_j)$ for all $j \leq p^e$ and since a polynomial has at most as many zeros as its degree, σ_j is identically zero for all $1 \leq j \leq p^e$.

Let c_j be coefficient of the term of degree $j(q-1)$ in the polynomial $\sigma_j(Y)$. Then

$$\prod_{x\in\mathcal{S}}(X-x_1^{q-1})=\sum_{j=0}^{q^{k-1}}c_jX^{q^{k-1}-j}=X^{q^{k-1}}+c_{p^e+1}X^{q^{k-1}-p^e-1}+\ldots+c_{p^{k-1}}.$$

Now $x_1\in\mathrm{GF}(q)$ and so $x_1^{q-1}=1$ unless $x_1=0$. If we write t for the number of points of $x\in\mathcal{S}$ with first coordinate zero then

$$\prod_{x\in\mathcal{S}}(X-x_1^{q-1})=X^t(X-1)^{q^{k-1}-t}=\sum_{j=0}^{q^{k-1}}\binom{-t}{j}(-1)^jX^{q^{k-1}-j}.$$

Comparing the above two equations we see that $\binom{-t}{p^r}=0$ modulo p for all $0\le r\le e$ and so $t=0$ mod p^{e+1}, by Lucas' Theorem. Thus the number of points of $\mathcal{S}$ incident with the hyperplane with first coordinate zero is 0 modulo p^{e+1}. However, this hyperplane was chosen arbitrarily among the hyperplanes that do not contain exactly q^{k-2} points of $\mathcal{S}$. Hence, every hyperplane is incident with 0 modulo p^{e+1} points of $\mathcal{S}$. □

Corollary 2.1. *Let $q=p^h$ and $1\le p^eq^t<q^{k-2}$, where $e,t\in\mathbb{Z}$. If there are more than $p^eq^t(q-1)$ directions not determined by a set $\mathcal{S}$ of q^{k-1} points in $AG(k,q)$ then every $(k-1-s)$-dimensional subspace, where $0\le s\le t$, meets $\mathcal{S}$ in 0 modulo $p^{e+1}q^{t-s}$ points.*

Proof. Let Σ_{k-1-s} be a $(k-1-s)$-dimensional subspace which does not contain q^{k-2-s} points of $\mathcal{S}$.

We first prove that there is a hyperplane containing Σ_{k-1-s} which does not contain exactly q^{k-2} points of $\mathcal{S}$. So we assume $s\ge 1$ since otherwise there is nothing to prove. If every subspace of dimension $k-s$ which contains Σ_{k-1-s} contains exactly q^{k-s-1} points of $\mathcal{S}$ then

$$|\mathcal{S}|=q^{k-1}=n+(q^{k-s-1}-n)(q^{s+1}-1)/(q-1),$$

where n is the number of points of $\mathcal{S}$ contained in Σ_{k-s-1}. This implies that $n=q^{k-1}$ which by assumption it is not. Therefore we can find a chain of subspaces $\Sigma_{k-s-1}\subset\Sigma_{k-s}\subset\ldots\subset\Sigma_{k-1}$ with the property that $|\mathcal{S}\cap\Sigma_{k-1}|\ne q^{k-2}$. Thus Σ_{k-1} meets the subspace at infinity in a subspace consisting entirely of determined directions.

There are $(q^k-q^{k-1})/(q^{k-s}-q^{k-s-1})=q^s$ subspaces of dimension $k-s$ that contain Σ_{k-1-s} and are not contained in Σ_{k-1} and so one of them meets the subspace at infinity in a subspace that contains at least $p^eq^{t-s}(q-1)$ non-determined directions. Applying Theorem 1.3 to this subspace, the corollary follows. □

3. Constructions

Let us first see that the bound in Theorem 1.3 is tight in the case $p^e=q^s$.

Proposition 3.1. *Let W and X be two subspaces of $PG(k,q)$ of dimension $s+1$ whose intersection is a subspace of dimension $s\ge 0$ and let U be a hyperplane containing W but not X. Let π be a hyperplane containing neither W nor X. Then the set of points $\mathcal{S}=((U\setminus W)\cup X)\setminus\pi$ of $PG(k,q)\setminus\pi$ has $q^s(q-1)=p^e(q-1)$ non-determined directions and there is a hyperplane incident with p^e modulo p^{e+1} points of $\mathcal{S}$.*

Proof. Let l be a line incident with exactly one point of $(\pi \cap \langle X, W\rangle) \setminus (X \cup W)$, where $\langle X, W\rangle$ denotes the subspace generated by X and W. We want to show that l is incident with exactly one point of $\mathcal{S}$. Since l is a line not contained in the hyperplane U it is incident with exactly one point P of U. If $P \in W$ then the line l is contained in $\langle X, W\rangle$ and so is incident with a point of X, since X is a hyperplane of $\langle X, W\rangle$. Note that l is not contained in X nor W. Thus l is incident with a unique point of $\mathcal{S}$. If $P \in U \setminus W$ then clearly l is not contained in $\langle X, W\rangle$ and so is not incident with a point of X. Thus every point of $(\pi \cap \langle X, W\rangle) \setminus (X \cup W)$ is a direction not determined by the set of points $\mathcal{S}$ and there are $(q^{s+2} - 1 - 2(q^{s+1} - 1) + q^s - 1)/(q - 1) = q^s(q - 1) = p^e(q - 1)$ of them. Moreover, the hyperplane U is incident with $q^{k-1} - q^{s+1} + q^s = p^e$ modulo p^{e+1} points of $\mathcal{S}$. □

The following construction is a more complicated generalisation of the previous one in which we view the points of $\mathrm{AG}(k, q)$, where $q = p^{eh}$, as points of $\mathrm{AG}(kh, p^e)$. Let π be a hyperplane of $\mathrm{PG}(kh, p^e)$. The subspaces of $\mathrm{AG}(k, q)$ of dimension 1 are subspaces of dimension h of $\mathrm{AG}(kh, p^e) \simeq \mathrm{PG}(kh, p^e) \setminus \pi$, and meet π in a spread of subspaces of dimension $h - 1$, which we shall call the Desarguesian spread and denote by $\mathcal{D}$. Any two elements of $\mathcal{D}$ span a subspace of dimension $2h-1$ which is partitioned by elements of $\mathcal{D}$.

Proposition 3.2. *Let U be a subspace of dimension $(k - 1)h$ of $AG(kh, p^e)$ and let W and X be subspaces of dimension t, where $(k - 1)h - 1 \geq t \geq h$, with the property that $W \subset U$ and $X \cap U \subset W$. Let $t + r$ be the dimension of $\langle X, W\rangle$ and let A be a subspace of dimension h which meets π in an element D of $\mathcal{D}$ that is skew from U and X and which intersects $\langle X, W\rangle$ in a subspace of dimension $r - 1$. Then A is incident with exactly one point of $\mathcal{S} = ((U \setminus W) \cup X) \setminus \pi$ and hence D is a direction not determined by $\mathcal{S}$ viewed as a subset of $AG(k, q)$.*

Proof. Since A has dimension h and it has a hyperplane D which is skew from U, the intersection $A \cap U$ is a point P. Let $B = A \cap \langle X, W\rangle$. Thus $B \supseteq D \cap \langle X, W\rangle$ and so its dimension is at least $r - 1$.

If $P \in U \setminus W$ then we need to show that $A \cap X = \emptyset$. If $A \cap X \neq \emptyset$ then the dimension of B is at least r. Now W and B are subspaces, of dimension t and at least r respectively, of $\langle X, W\rangle$ which has dimension $t + r$. Thus there is a point Q in their intersection which, since $B \subseteq A$, is a point of $A \cap W \subseteq A \cap U$. Hence $Q = P \in W$, a contradiction.

If $P \in W$ then we need to show that $A \cap X$ is a point. Since D, a hyperplane of A, has an intersection with $\langle X, W\rangle$ of dimension $r - 1$ and $P \in A \setminus D$, the dimension of B is at least r. Now X and B are subspaces, of dimension t and at least r respectively, of $\langle X, W\rangle$ which has dimension $t + r$. Thus there is a point Q in their intersection which, since $B \leq A$, is a point of A. If $A \cap X$ contains a line then, since D is a hyperplane of A, there is a point in the intersection $D \cap X$, which there is not by assumption. Thus $A \cap X = \{Q\}$. □

In general it is of course dependent on U, X and W how many elements D have the property that it is skew from U, X and W and intersects $\langle X, W\rangle$ in a subspace of dimension $r - 1$. Recall that D is a subspace of dimension $h - 1$, so $1 \leq r \leq h$.

In the case $r = 1$ we can count the number of directions not determined by $\mathcal{S}$. Any spread element $D \in \mathcal{D}$ that intersects $(\langle X, W\rangle \cap \pi)$ and is skew from $\langle U\rangle$ and $\langle X\rangle$, meets it in a point since it has no non-trivial intersection with $\langle W\rangle$. Note that elements of $\mathcal{D}$ are either completely contained in $\langle U\rangle$ or disjoint. The number of points in $(\langle X,W\rangle\cap\pi)\setminus\{\langle X,W\rangle\}$ is $p^{et}-p^{e(t-1)}$.

Let us show that for $r=1$ we can choose U, W and X with $t=h+1$ in such a way that there is a hyperplane H of $AG(k,p^{eh})$ incident with p^e modulo p^{2e} points of $\mathcal{S}$. The paragraph before implies that there are p^eq-q directions not determined by $\mathcal{S}$. Let U be a subspace of dimension $kh-h$ of $\mathrm{AG}(kh,p^e)$ which corresponds to a hyperplane of $\mathrm{AG}(k,p^{eh})$ and let $G\subset U$ be a subspace of dimension $kh-2h$ of $\mathrm{AG}(kh,p^e)$ which corresponds to a subspace of dimension $k-2$ of $\mathrm{AG}(k,p^{eh})$. Choose X so that the dimension of $X\cap G$ is 1 and W so that the dimension of $W\cap G$ is 2. This is easily done since $W\subset U$ and the dimension of W is $h+1$ and the dimension of $X\cap U$ is h. The set $X\setminus U$ as a subset of $\mathrm{AG}(k,p^{eh})$ consists of $p^{e(h+1)}-p^{eh}$ points. A hyperplane that contains G and is incident with a point of $X\setminus U$ is incident with a multiple of p^e points of $X\setminus U$. Hence there are at most $p^{eh}-p^{eh-e}<p^{eh}$ hyperplanes containing G and incident with points of $X\setminus U$. Thus there is a hyperplane H which meets X only in the p^e points $X\cap U$. This hyperplane meets W in p^{2e} points and U in $p^{(k-2)eh}$ points and so is incident with p^e modulo p^{2e} points of $\mathcal{S}$.

We can make good examples with lots of non-determined directions from examples in smaller dimensions, which have a lot of non-determined directions, in the following way. Let us suppose we have a set of q^{k-2} points $\mathcal{S}_0$ in $\mathrm{AG}(k-1,q)$, a hyperplane incident with $b\neq 0$ modulo p^{e+1} points, and let $\mathcal{N}_0$ be the set of non-determined directions. Embed the affine space in $\mathrm{AG}(k,q)$ and choose a point at infinity P that is not in the subspace spanned by $\mathcal{S}_0$. Let $\mathcal{S}$ be the cylinder (a cone with vertex at infinity) formed by taking as the vertex the point P and as the base the set $\mathcal{S}_0$. Then $\mathcal{S}$ is a set of q^{k-1} points of $\mathrm{AG}(k,q)$ and every point on a line joining an element of $\mathcal{N}$ to the point P (except the point P) is a non-determined direction of the set $\mathcal{S}$. Thus $\mathcal{S}$ has $|\mathcal{N}|q$ non-determined directions and there is a hyperplane incident with bq modulo $p^{e+1}q$ points of $\mathcal{S}$.

4. Ovoids of parabolic quadrics

Theorem 1.3 allows us to shorten yet further the proof that ovoids of $\mathrm{Q}(4,p)$ are elliptic quadrics, which was first proven in [2]. Let us first briefly recall what an ovoid of $\mathrm{Q}(4,p)$ is. The generalised quadrangle $\mathrm{Q}(4,p)$ consists of points, the singular points of a non-degenerate quadratic form f in five variables, and lines, the totally isotropic lines with respect to the form. A maximal subset $\mathcal{O}$ of the points of $\mathrm{Q}(4,p)$ with the property that for all $x,y\in\mathcal{O}$, $x\neq y$, $\beta(x,y)\neq 0$, where β is the symmetric bilinear form associated with f, is called an *ovoid* of $\mathrm{Q}(4,p)$.

Theorem 1.3 with $h=1$, $k=3$ and hence $e=0$ implies that every plane is incident with 0 modulo p points of a set of p^2 points of $\mathrm{AG}(3,p)$ whose non-determined directions contain a conic (and so there are at least $p+1$ of them). Such a set of points corresponds to an ovoid of $\mathrm{Q}(4,p)$ and the plane intersection property implies that every hyperplane of $\mathrm{PG}(4,p)$ that intersects $\mathcal{O}$, intersects $\mathcal{O}$ in 1 modulo p points, see [2].

Let τ_i be the number of hyperplanes of $\mathrm{PG}(4,p)$ that are incident with i points of $\mathcal{O}$. Klaus Metsch points out that for an elliptic quadric

$$\sum_{i=0}^{p^2+1}(p^2+1-i)(p+1-i)(i-1)\tau_i = 0,$$

and since we can count $\sum i\tau_i$, $\sum i^2\tau_i$ and $\sum i^3\tau_i$ for any ovoid this sum must be zero for all ovoids. Theorem 1.3 implies that $\tau_i = 0$ unless $i = 0$ or congruent to 1 modulo p so all terms in the sum are negative or zero and hence zero. Thus every hyperplane meets the ovoid in 1, $p+1$ or p^2+1 points.

Suppose that there does not exist a hyperplane containing p^2+1 points of $\mathcal{O}$. Then all hyperplanes intersect $\mathcal{O}$ in either 1 or $p+1$ points. Let π be any plane incident with $x > 2$ points of $\mathcal{O}$ and count the points of $\mathcal{O}$ on the hyperplanes containing π. Then

$$p^2+1 = x + (p+1)(p+1-x),$$

hence $x = 2$, a contradiction. So there is a hyperplane intersecting $\mathcal{O}$ in p^2+1 points, all of whose points are elements of $\mathcal{O}$. Such a set is an elliptic quadric.

5. The cylinder conjectures

Theorem 1.3 has led to some conjectures being formulated. In $\mathrm{AG}(3,p)$ the only way we know to form sets of p^2 points with many directions not determined is to form a cylinder from a point set in $\mathrm{AG}(2,q)$ that has some non-determined directions. Indeed the *weak cylinder conjecture* is the following.

Conjecture 5.1. *Let $\mathcal{S}$ be a set of p^2 points in $AG(3,p)$ and let $\mathcal{N}$ be the set of non-determined directions. If $|\mathcal{N}| \geq q$ then $\mathcal{S}$ is the union of p parallel lines.*

Since Theorem 1.3 implies that such a set $\mathcal{S}$ must have the property that every hyperplane is incident with 0 modulo p points of $\mathcal{S}$ we can weaken the hypothesis and form the *strong cylinder conjecture* (which implies the weak version).

Conjecture 5.2. *Let $\mathcal{S}$ be a set of p^2 points in $AG(3,p)$. If $\mathcal{S}$ has the property that every plane is incident with 0 modulo p points of $\mathcal{S}$ then $\mathcal{S}$ is the union of p parallel lines.*

There are various ways to generalise these conjectures to higher dimensional spaces. Equally there are various ways to generalise the following formulation of the strong cylinder conjecture which is given in terms of abelian groups.

Conjecture 5.3. *Let G be an elementary abelian p-group of size p^3 and let S be a set of p^2 elements of G. If every coset of size p^2 contains 0 modulo p elements of S then S is the union of cosets of the same subgroup of size p.*

References

[1] S. Ball, The number of directions determined by a function over a finite field, *J. Combin. Theory Ser. A*, **104** (2003) 341–350.

[2] S. Ball, P. Govaerts and L. Storme, On ovoids of parabolic quadrics, *Des. Codes Cryptogr.*, 38 (2006) 131–145.

[3] S. Ball and M. Lavrauw, How to use Rédei polynomials in higher dimensional spaces, *Le Matematiche (Catania)*, **59** (2004) 39–52.

[4] S. Ball and M. Lavrauw, On the graph of a function in two variables over a finite field, *J. Algebraic Combin.*, **23** (2006) 243–253.

[5] A. Blokhuis, S. Ball, A. E. Brouwer, L. Storme and T. Szőnyi, On the number of slopes of the graph of a function defined over a finite field, *J. Combin. Theory Ser. A*, **86** (1999) 187–196.

[6] L. Storme and P. Sziklai, Linear point sets and Rédei type k-blocking sets in $\mathrm{PG}(n, q)$, *J. Algebraic Combin.*, **14** (2001) 221–228.