On the number of solutions of polynomial systems

M.Boguslavsky

February 25, 1996

Abstract. We consider systems of homogenous polynomial equations of degree d in a projective space $\mathbb{P}^m$ over a finite field $\mathbb{F}_q$. We are trying to determine the maximum possible number of solutions of such systems. The complete answer for the case $r = 2$, $d < q - 1$ is given, as well as new conjectures about the general case. We also prove a bound on the number of points of an algebraic set of given codimension and degree.

We also discuss an application of our results to coding theory, namely to the problem of computing generalized Hamming weights for q-ary projective Reed-Muller codes.

1 Introduction

Consider a system of polynomial equations

$$\begin{cases} F_1(x_0 : x_1 : \ldots : x_m) &= 0 \\ F_2(x_0 : x_1 : \ldots : x_m) &= 0 \\ \qquad\qquad \ldots & \\ F_r(x_0 : x_1 : \ldots : x_m) &= 0 \end{cases} \tag{1}$$

where F_i are linearly independent homogenous polynomials in $m+1$ variables over a finite field $\mathbb{F}_q$ with q elements. Suppose all F_i have degree d. The main purpose of this paper is to determine the maximal possible number of solutions of system (1) in m-dimensional projective space $\mathbb{P}^m$ $(\mathbb{F}_q)$.

In this paper q is fixed, $|X|$ denotes the number of $\mathbb{F}_q$-points of an algebraic set X, $p_m = |\mathbb{P}^m| = \frac{q^{m+1}-1}{q-1}$.

The case of one equation ($r = 1$) was considered a few years ago. M.Tsfasman constructed for each $d \leq q+1$ a polynomial F of degree d with $dq^{m-1} + p_{m-2}$ zeroes and made a conjecture that this is the maximal possible value. This was proved by J.-P. Serre [11] and by Sørensen [12], [13].

Theorem 1 *Let $F(x_0 : x_1 : \ldots : x_m)$ be a homogenous polynomial in $m + 1$ variable with coefficients in $\mathbb{F}_q$ and of degree d. The number of zeroes of $F(x_0 : x_1 : \ldots : x_m)$ in $\mathbb{P}^m$ $(\mathbb{F}_q)$ is less than or equal to $dq^{m-1} + p_{m-2}$.*

[0]This work was supported in part by the International Science Foundation under grants MPN000 and MPN300 and by the Russian Basic Research Foundation grant 96-01-01378

Serre used the induction on the dimension m to prove that the number of zeroes of Tsfasman's polynomial F is the maximal possible. F is a reducible polynomial. The zeroset X of this polynomial is a union of d hyperplanes passing through one common linear space of codimension 2.

Thus the bound given by Theorem 1 is exact for $d \leq q+1$. When $d = q+1$ the theorem gives the upper bound p_m. For $d \geq q+1$ there exist polynomials with p_m zeroes.

One can study the same problem from another point of view. Let us consider the Veronese embedding of degree d $\quad \mathcal{V}_d : \mathbb{P}^m \to \mathbb{P}^{\binom{d+m}{m}-1}$. For $i_0 + i_1 + \ldots + i_m = d$ denote the homogenous coordinates in $\mathbb{P}^{\binom{d+m}{m}-1}$ by $(u_{i_0 i_1 \ldots i_m})$, and let $x_0, \ldots, x_m$ be the homogenous coordinates in $\mathbb{P}^m$. The Veronese embedding is the map given by $u_{i_0 i_1 \ldots i_m} = x_0^{i_0} x_1^{i_1} \ldots x_m^{i_m}$. The image of $\mathbb{P}^m$ under this map is called a Veronese variety. Any hyperplane section of a Veronese variety is a 1-1 image of an effective divisor of degree d in $\mathbb{P}^m$. Therefore any section of a Veronese variety by a linear subspace of codimension r is a 1-1 image of an intersection of r independent effective divisors of degree d in $\mathbb{P}^m$. Thus the study of solutions of system (1) is equivalent to the study of linear sections of Veronese varieties.

Suppose $r = 2$. Then system (1) consists of 2 equations. In section 3 we prove the following theorem.

Theorem 2 *Let $F_1(x_0 : x_1 : \ldots : x_m)$ and $F_2(x_0 : x_1 : \ldots : x_m)$ be homogeneous polynomials in $m+1$ variables of degree d. Suppose they are linearly independent and $d < q-1$; then the maximal possible number of their common zeroes in $\mathbb{P}^m$ $(\mathbb{F}_q)$ equals $(d-1)q^{m-1} + p_{m-2} + q^{m-2}$.*

Theorem 2 is a direct modification of Theorem 1 to the case $r = 2$. The proof uses similar ideas.

To prove Theorem 2 we need the following Theorem 3, which can be also considered as a bound for the number of solutions of system (1) when polynomials F_i are supposed to have no common proper divisors.

Theorem 3 *Let $X \subset \mathbb{P}^m$ be an algebraic set of degree δ and dimension s. Then*

$$|X| \leq \delta p_s.$$

For $\delta \leq q$ Theorem 3 was proven by Lachaud [6]. This bound is far better than the bound of Schmidt (see [10], Lemma 4.)

Now we give some definitions. The set of solutions of system (1) is called an (r, m, d)-*configuration* , corresponding to system (1). An (r, m, d)-configuration is always an algebraic subset in $\mathbb{P}^m$ whose image under the Veronese embedding of degree d lies in a linear subspace of codimension r.

Note that a given subset of $\mathbb{P}^m$ can be an (r, m, d)-configuration for many different r and d.

An (r, m, d)-configuration is called *maximal,* if it contains the maximum possible number of $\mathbb{F}_q$-points (for given r, m, d and q).

An (r, m, d)-configuration X is called linear if all $\mathbb{F}_q$-points lie on linear components of X. Note that there can be non-linear components which contribute no extra $\mathbb{F}_q$-points.

A linear (r, m, d)-configuration is called *dim-maximal* , if it contains the maximal possible number of components of high dimension (a strict definition is given in the next section).

In section 3, we construct a maximal $(2, m, d)$-configuration, which consists of a maximal $(1, m, d-1)$-configuration and of an additional linear subspace of codimension 2. This configuration as well as a maximal $(1, m, d)$-configuration is linear and dim-maximal. WE make a conjecture that a maximal (r, m, d)-configuration is also linear and dim-maximal. This will be discussed in section 2. In section 3, we also prove Theorems 2 and 3. Applications to the coding theory are given in section 4.

This work was presented in part at the conference 'Algebraic and Combinatorial Coding Theory', Novgorod, Russia, September 1994 and at the colloquium "Arithmetic, Geometry & Coding Theory", C.I.R.M. Luminy, Marseille, France, June 1995.

The author is grateful to M.Tsfasman for putting the problem and for his constant attention to this work.

2 Conjectures

We know that in the affine case all maximal $(1, m, d)$-configurations are linear (see [7] for the binary case and [2] for arbitrary q).

The following conjecture was stated by M.Tsfasman.

Conjecture 1 *There exists a maximal (r, m, d)-configuration which is linear.*

By Theorem 1 and 2, this conjecture is true for $r = 1, 2$.

Now we introduce the notion of a dim-maximal linear (r, m, d)-configuration .

Let us consider linear (r, m, d)-configurations from the point of view of dimensions of their components. We shall say that $(\nu_1, \nu_2, \ldots, \nu_m)$ is the *dim-type* of a linear (r, m, d)-configuration X if for all $i = 1, \ldots, m$, X contains ν_i components of codimension i not contained in components of smaller codimensions.

The lexicographical order on the dim-types induces a linear order on the set of all linear (r, m, d)-configurations : a configuration containing ν_i components defined over $\mathbb{F}_q$ for all $i = 1, \ldots, m$ is greater than a configuration

containing μ_i components of codimension i for all $i = 1, \ldots, m$, if and only if there exists b such that $\nu_i = \mu_i$ for any $i < b$ and $\nu_b > \mu_b$.

An (r, m, d)-configuration that is maximal with the respect to this order is called dim-maximal.

The following conjecture looks also plausible to us.

Conjecture 2 *Let $x_1^{\nu_1} x_2^{\nu_2} \ldots x_{m+1}^{\nu_{m+1}}$ be the r-th in lexicographical order monomial of degree d in $m+1$ variable. Then the dim-type of a dim-maximal configuration is $(\nu_1, \nu_2, \ldots, \nu_m)$.*

Note that for an arbitrary configuration the sum $\sum_i \nu_i$ can exceed d.

Now we shall give another expression for the set $\{\nu_i(r), i = 1 \ldots m+1\}$. Let $x_1^{\nu_1} x_2^{\nu_2} \ldots x_{m+1}^{\nu_{m+1}}$ be the r-th monomial. For each j_1 ($\nu_1 < j_1 \leq d$) there exist $\binom{d-j_1+m-1}{m-1}$ monomials starting with $x_1^{j_1}$. All these monomials precede $x_1^{\nu_1} x_2^{\nu_2} \ldots x_{m+1}^{\nu_{m+1}}$. Further, for each j_2 ($\nu_2 < j_2 \leq d - \nu_1$) there exist $\binom{d-\nu_1-j_2+m-2}{m-2}$ monomials starting with $x_1^{\nu_1} x_2^{j_2}$. They also precede $x_1^{\nu_1} x_2^{\nu_2} \ldots x_{m+1}^{\nu_{m+1}}$. Similarly, for each i ($1 \leq i \leq m+1$) and for each j_i ($\nu_i < j_i \leq d - \sum_{l=1}^{i-1} \nu_l$) there exist $\binom{d-\sum_{l=1}^{i-1}\nu_l - j_i + m - i}{m-i}$ monomials that start with $x_1^{\nu_1} x_2^{\nu_2} \ldots x_i^{j_i}$ and precede the monomial $x_1^{\nu_1} x_2^{\nu_2} \ldots x_{m+1}^{\nu_{m+1}}$. Therefore

$$r = \sum_{i=1}^{m+1} \sum_{j=\nu_i+1}^{d-\sum_{l=1}^{i-1}\nu_l} \binom{d - \sum_{l=1}^{i-1} \nu_l - j + m - i}{m-1}. \tag{2}$$

Lemma 4 *There exists a union of d_i linear subspaces of $\mathbb{P}^m$ of codimension i ($i = 1, \ldots, m$) that contains*

$$\sum_{i=j}^{m} d_i (p_{m-i} - p_{m-i-j}) + p_{m-2j}$$

$\mathbb{F}_q$-points, where j is the smallest integer such that $d_j \neq 0$. This is the maximum possible number of points on a union of d_i linear subspaces of codimension i ($i = 1, \ldots, m$).

Proof. We compute the maximal possible number of $\mathbb{F}_q$-points on a union X of d_1 linear subspaces Π_ℓ^{m-1} ($\ell = 1 \ldots d_1$) of codimension 1, d_2 linear subspaces Π_ℓ^{m-2} ($\ell = 1 \ldots d_2$) of codimension 2, $\ldots$, d_m linear subspaces Π_ℓ^0 ($\ell = 1, \ldots, d_m$) of codimension m. We have

$$|X| = \sum_i d_i p_{m-i} - |I|,$$

where I is a set of points (with multiplicities) that were counted more than once; a point P belongs to I with multiplicity t iff P belongs exactly to $t+1$

linear subspaces Π_ℓ^i. A configuration with the maximal number of points is a configuraton with the minimal number of points in I.

Let j be the smallest integer such that $d_j > 0$. Fix a linear subspace Π_1^{m-j}. Each linear subspace of codimension i intersects with Π_1^{m-j} at least by a space of codimension $i+j$. Thus,

$$|I| \geq (d_j - 1)p_{m-j} + \sum_{i=j+1}^{m} d_i p_{m-i-j} = \sum_{i=j}^{m} d_i p_{m-i-j} - p_{m-2j}.$$

Now we prove that there exists a configuration with $|I| = \sum_{i=j}^{m} d_i p_{m-i-j} - p_{m-2j}$. Put all components of minimal codimension j so that they intersect by one common linear subspace M of codimension $2j$ in $\mathbb{P}^m$. Since $d_j \leq q$, we can put all components of codimension $j+1$ so that they do not intersect with any of Π_ℓ^{m-j} outside M, $\Pi_i^{m-j-1} \cap \Pi_\ell^{m-j-1} \subset M$ $(i \neq \ell)$, and the dimensions of intersections $\Pi_i^{m-j-1} \cap \Pi_\ell^{m-j-1}$ and $\Pi_i^{m-j-1} \cap \Pi_\ell^{m-j}$ are maximal. Since $d_{j+1} \leq q$, we can put all components of codimension $j+2$ so that all intersections $\Pi_i^{m-j-2} \cap \Pi_\ell^{m-j}$, $\Pi_i^{m-j-2} \cap \Pi_\ell^{m-j-1}$ and $\Pi_i^{m-j-2} \cap \Pi_\ell^{m-j-2}$ $(i \neq \ell)$ have maximum dimensions and are contained in M, etc. Finally, put all linear subspaces of codimension m (points) outside all other components. It is easy to check that I contains exactly $\sum_{i=j}^{m} d_i p_{m-i-j} - p_{m-2j}$ points. Therefore the configuration contains the maximal number of points. $\lhd$

We propose the following

Conjecture 3 *There exists a maximal (r, m, d)-configuration that is dim-maximal.*

We know that this conjecture is true for $r = 1, 2$ and for the plane case ($m = 2$). Clearly, a dim-maximal (1,m,d)-configuration contains d hyperplanes, so the maximal (1,m,d)-configuration described in section 1 is dim-maximal. In the proof of Lemma 6, we construct a maximal (2,m,d)-configuration. It contains $d-1$ hyperplanes and one linear subvariety of $\mathbb{P}^m$ of codimension 2 outside these hyperplanes. It is readily seen that this configuration is also dim-maximal.

After this work has been written, the author discovered the paper [4] where the affine case is considered. Their maximal affine configuration is alike configuration from Conjecture 3. The method of the proof is quite different and it is not clear how it can be extended to the projective case.

From Lemma 4 easily follows the

Corollary 5 *Suppose Conjecture 3 holds, then the maximum possible number of points on an (r, m, d)-configuration equals*

$$\sum_{i=j}^{m} \nu_i (p_{m-i} - p_{m-i-j}) + p_{m-2j},$$

where ν_i are such that $x_1^{\nu_1}x_2^{\nu_2}\dots x_{m+1}^{\nu_{m+1}}$ is the r-th (in lexicographical order) monomial of degree d in $m+1$ variables and j is the smallest integer such that $\nu_j \neq 0$.

In 1995, Lachaud proposed the following conjecture.

Conjecture 4 *Under the conditions of Theorem 3 suppose that $s \geq m/2$ and $d \leq q+1$. Then*

$$|X| \leq \delta p_s - (\delta - 1)p_{2s-m}.$$

For relevant δ and s this conjecture is stronger than Theorem 3. By Lemma 4, this conjecture holds for a union of linear subvarieties. Moreover, Lemma 4 implies that if this conjecture is true then its bound is exact.

3 Two equations

In this section we prove Theorems 2 and 3. Let R and S denote divisors of zeroes of functions F_1 and F_2 respectively. Let us show that if Theorem 2 holds, its bound is exact.

Lemma 6 *There exist effective divisors R and S of degree d such that*

$$|R \cap S| = (d-1)q^{m-1} + q^{m-2} + p_{m-2}.$$

Proof. Let $H_1, \dots, H_{d-1}$ be $d-1$ hyperplanes with a common linear space M of codimension 2. Let N be a linear subspace of codimension 2 such that N intersects M by a linear subspace of codimension 3 and is not contained in any of H_i. Then N doesn't intersect any of H_i outside M. Let H_d and H'_d be any pair of hyperplanes intersecting by N. Let $R = H_1 + H_2 + \dots + H_d$ and $S = H_1 + H_2 + \dots + +H_{d-1} + H'_d$. Obviosly,

$$|R \cap S| = (d-1)|H_1 \backslash M| + |N \backslash M| + |M| = (d-1)q^{m-1} + q^{m-2} + p_{m-2}.$$

$\lhd$

Theorem 3 gives a bound on the number of $\mathbb{F}_q$-points in an algebraic set X of dimension s and degree δ in $\mathbb{P}^m$. The bound does not depend on m. This topic was discussed by Lachaud in [6]. Lachaud proved that if $\delta \leq q$ then there exists a linear subspace of dimension $m-s-1$ in $\mathbb{P}^m$ defined over $\mathbb{F}_q$ that doesn't intersect X, the projection of X from this subspace is a δ-sheeted covering of $\mathbb{P}^s$ defined over $\mathbb{F}_q$, so

$$|X| \leq \delta p_s. \tag{3}$$

This bound can be easily improved when $\delta \geq p_m/p_s$: the number of $\mathbb{F}_q$-points on X can not exceed p_m. The problem of exactness of the bound of Theorem 3 for $\delta < p_m/p_s$ will be discussed in another paper.

Proof of Theorem 3.

The proof is by induction on m. For $m = 1$ we have $\dim X = 0$ and $|X| \leq \deg X = \delta$. Suppose we proved the theorem for the dimension $m-1$.

First we consider the case (I) when X is irreducible and not contained in a hyperplane. Secondly we consider the case (II) when X is contained in a hyperplane. Finally (III), we deduce from (I) and (II) the bound for an arbitrary X.

(I) Suppose X is irreducible and X is not contained in any hyperplane. Thus, $X \cap H$ is an algebraic set of dimension $s-1$ and degree δ in $H \simeq \mathbb{P}^{m-1}$ for any hyperplane H. By the induction hypothesis, $|X \cap H| \leq \delta p_{s-1}$.

Now we use a construction, similar to one Serre used to prove Theorem 1. Consider the set in $\mathbb{P}^{m*} \times \mathbb{P}^m$ consisting of all pairs (H, P), where H is a hyperplane and P a point of $\mathbb{P}^m$, both defined over $\mathbb{F}_q$, such that $P \in H \cap X$. We compute the number of $\mathbb{F}_q$-points in this set by two different ways.

We have $|X|$ ways of selecting a point $P \in X$ and for each P we have p_{m-1} ways of selecting H. On the other hand, we can first select one of p_m hyperplanes in $\mathbb{P}^m$ and then select one of points on the intersection $H \cap X$. So,

$$|X|p_{m-1} = \sum_H |H \cap X| \tag{4}$$

Combining this with

$$|H \cap X| \leq \delta p_{s-1},$$

we get

$$|X|p_{m-1} \leq p_m \delta p_{s-1}.$$

Thus,

$$|X| \leq \delta p_s \frac{p_{s-1}p_m}{p_s p_{m-1}}.$$

The reader will easily prove that $\frac{p_{s-1}p_m}{p_s p_{m-1}} < 1$, so

$$|X| < \delta p_s. \tag{5}$$

(II) Suppose X is contained in a hyperplane H. Then X is an algebraic set of dimension s in $H \simeq \mathbb{P}^{m-1}$ and of degree δ . By the induction hypothesis,

$$|X| \leq \delta p_s. \tag{6}$$

(III) Let X be an arbitrary algebraic set of dimension s. X can be decomposed into the sum of (absolutely) irreducible components $X = X_1 + X_2 + \ldots + X_k$ of degrees $\delta_1, \delta_2 \ldots \delta_k$; $\sum_{i=1}^k \delta_i = \delta$. If X_i is not contained in a hyperplane then $|X_i| \leq \delta_i p_s$ by inequality (5). If X_i is contained in a

hyperplane the same is true by inequality (6). Note that some of X_i may be not defined over $\mathbb{F}_q$, some of them may have dimension less than s; in both cases we have the same bound.

Thus,

$$|X| \leq \sum_{i=1}^{k} |X_i| \leq (\sum_{i=1}^{k} \delta_i) p_s = \delta p_s.$$

$\lhd$

Now we prove Theorem 2. Let $M_q(2, m, d)$ denote the number of points on the configuration from Lemma 6: $M_q(2, m, d) = (d-1)q^{m-1} + q^{m-2} + p_{m-2}$. We show that for any two effective divisors R and S of degree d in $\mathbb{P}^m$

$$|R \cap S| \leq M_q(2, m, d).$$

Proof of Theorem 2.

(I) Let X be the intersection $R \cap S$ and let Y be the maximal divisor such that $R - Y \geq 0$ and $S - Y \geq 0$. Let X' be $(R-Y) \cap (S-Y)$. Then $X = Y \cup X'$. Let $b = \deg Y$. Then $0 \leq b \leq d-1$. By Theorem 1, $|Y| \leq bq^{m-1} + p_{m-2}$. X' is an algebraic set of codimension 2 and degree $\delta = (d-b)^2$. By Theorem 3, $|X'| \leq (d-b)^2 p_{m-2}$.

(II) Suppose $b = 0$, then $X = X'$ and $|X| \leq d^2 p_{m-2}$. It can easily be checked that

$$|X| - M_q(2, m, d) \leq \frac{d-1}{q-1} \left(-q^m + (d+2)q^{m-1} - (d+1) \right) - q^{m-2}.$$

For $d < q - 1$ the last expression is negative, so $|X| \leq M_q(2, m, d)$.

(III) Suppose $b > 0$. We have

$$|X| \leq |Y| + |X'| \leq bq^{m-1} + p_{m-2} + (d-b)^2 p_{m-2}.$$

After some calculations we get

$$|X| - M_q(2, m, d) \leq -\frac{1}{q-1} \left(q^{m-1} (d-b-1) (q - (d-b+2)) + (d-b)^2 - q^{m-2} \right) \tag{7}$$

The sign of the right hand side of (7) is the same as the sign of

$$\theta = -q^{m-1} (d-b-1) (q - (d-b+2)) - (d-b)^2 + q^{m-2}.$$

(IV) Suppose $0 < b < d-1$. If $(d-b-1)(q-(d-b+2)) > 0$ then

$$q^{m-1} (d-b-1) (q - (d-b+2)) \geq q^{m-1}$$

and $\theta < 0$. We have $d - b - 1 > 0$, $d - b \leq d - 1$. Combining this with the assumption $d < q - 1$ we get $d - b < q - 2$ and $(d-b-1)(q-(d-b+2)) > 0$.

Thus, $\theta < 0$ and $|X| \le M_q(2, m, d)$.

(v) Now we consider the last case $b = d - 1$. We have $\deg X' = 1$, so X' is a linear subspace of codimension 2. We can not apply Theorem 1 directly, since we would get

$$|X| \le |Y| + |X'| \le (d-1)q^{m-1} + p_{m-2} + p_{m-2} > (d-1)q^{m-1} + q^{m-2} + p_{m-2}.$$

If Y contains an $\mathbb{F}_q$-hyperplane H then $H \cap X'$ contains a linear subspace of dimension $m-3$, whence

$$|X| \le |Y| + |X'| - p_{m-3} \le (d-1)q^{m-1} + p_{m-2} + p_{m-2} - p_{m-3} = (d-1)q^{m-1} + q^{m-2} + p_{m-2}.$$

Suppose Y does not contain an $\mathbb{F}_q$-hyperplane, i.e. for any H the intersection $Y \cap H$ is a divisor on H. As in the proof of Theorem 3, we use the induction on the dimension m and Serre's construction.

The case $m = 1$ is trivial. Now suppose we proved the proposition for the dimension $m-1$. If $Y(\mathbb{F}_q) \subset X'$ then the proposition is evident. Otherwise fix an $\mathbb{F}_q$-point $Q \in (Y \backslash X')$. There exists a unique hyperplane H_0 passing through Q and X'. The intersection $H_0 \cap Y$ is a divisor of degree $d-1$ in $H \simeq \mathbb{P}^{m-1}$, $H_0 \cap X' = X'$. We have

$$|H_0 \cap X| \le |H_0 \cap Y| + |X'| \le (d-1)q^{m-2} + p_{m-3} + p_{m-2}.$$

For any other hyperplane $H \ne H_0$ passing through Q the intersection $H \cap X$ is an algebraic set in $H \simeq \mathbb{P}^{m-1}$ consisting of an effective divisor $H \cap Y$ of degree $d-1$ and of a linear subspace $H \cap X'$ of codimension 2 in H. By the induction hypothesis,

$$|H \cap X| \le M_q(2, m-1, d).$$

Consider the set in $\mathbb{P}^{m*} \times \mathbb{P}^m$ consisting of all pairs (H, P), where H is a hyperplane and P a point of $\mathbb{P}^m$, both defined over $\mathbb{F}_q$, such that $Q \in H$, $P \in H \cap X$, $P \ne Q$. We compute the number of $\mathbb{F}_q$-points in this set by two different ways.

We have $|X| - 1$ ways of selecting a point $P \in X$ such that $P \ne Q$ and for each P we have p_{m-2} ways of selecting H passing through P and Q. On the other hand, we can first select one of p_{m-1} hyperplanes in $\mathbb{P}^m$ passing through Q and then select one of points in $(H \cap X) \backslash Q$.

Thus,

$$(|X| - 1)p_{m-2}k = \sum_{H \ne H_0} (|H \cap X| - 1) + |H_0 \cap X| - 1 \quad \le$$
$$p_{m-1}\left(M_q(2, m-1, d) - 1\right) + p_{m-2} - q^{m-3}.$$

Therefore,

$$\begin{aligned} |X| &\leq 1 + \frac{p_{m-1}}{p_{m-2}} \left(M_q(2, m-1, d) - 1\right) + \frac{p_{m-2} - q^{m-3}}{p_{m-2}} \\ &= M_q(2, m, d) + \frac{1}{p_{m-2}} \left(q^{m-2}(d - 1 - q) + p_{m-3}\right). \end{aligned}$$

We have $d \leq q$; thus, $q^{m-2}(d-1-q) + p_{m-3} < 0$ and $|X| < M_q(2, m, d)$. This completes the proof of the theorem. $\lhd$

4 Generalized weights

In this section we discuss applications of our results to coding theory. A linear k-dimensional subspace C of $\mathbb{F}_q^n$ is called a *linear* $[n, k]_q$*-code*. Elements of this subspace are called *codewords* and n is called the *length* of C. The most important parameters of a linear code C are n, k and the *minimum Hamming distance* d.

Definition. The *support* $\chi(D)$ of a code D is defined as

$$\chi(D) = \{i : \exists (x_1, x_2, \ldots, x_n) \in D : x_i \neq 0\}.$$

The r-th *generalized Hamming weight* of a linear code C is the minimal support size of a r-dimensional subcode of C:

$$d_r(C) = min\{|\chi(D)| : D \subset C, \dim D = r\}.$$

Generalized weights of a linear $[n, k, d]_q$-code are a monotone set of integers $d_1 = d \leq d_2 \leq \ldots \leq d_{k-1} \leq d_k = n$. The set of all generalized weights $\{d_1, d_2, \ldots, d_k\}$ is called the *weight hierarchy* of a code.

Generalized weights first appeared in the paper [3]. Several applications of weight hierarchy are described in [17]. More information about generalized weights and the bibliography can be found in the survey paper by Tsfasman and Vlăduţ[15].

Hirschfeld, Tsfasman and Vlăduţ[5] presented a geometric interpretation of generalized weights. It is well known [14] that the study of linear $[n, k]_q$-codes can be reduced to the study of projective systems, that is of n-point subsets of a $(k-1)$-dimensional projective space over $\mathbb{F}_q$.

The minimum distance equals the minimal number of points of a projective system lying outside a hyperplane and the r-th generalized weight equals the minimal number of points outside a linear subspace of codimension r:

$$d_r = \min(|X| - |X \cap H|), . \tag{8}$$

The linear subspaces that reach the minimum in Eq.(8) contain the maximal possible number of points of the projective system X and are called the *maximal sections* of X.

Sets of $\mathbb{F}_q$-points of algebraic varieties are a good source of projective systems (see [14]). Codes, corresponding to algebraic varieties, are called algebraic-geometric codes.

Generalized weights for codes on several classes of algebraic varieties have been computed (see [5], [8], [9], [1] and [15] for more references.)

Veronese varieties correspond to q-ary projective Reed-Muller codes. These codes are one of natural generalizations of binary Reed-Muller codes. The minimal distance for these codes was computed in [12], [13].

In his paper [16], V.Wei computed the weight hierachy for binary Reed-Muller codes. He implemented a strong result from the extremal set theory, namely the Kruskal-Katona theorem. Note that in binary case d is always not less than $q = 2$, while our results concern the case $d < q$ and $q > 2$.

Heijnen and Pelikaan [4] recently computed the weight hierarchy for affine q-ary Reed-Muller codes. The answer is alike Corollary 8.

The following is a straightforward consequence of Theorem 2.

Corollary 7 *The second generalized Hamming weight of a projective q-ary Reed-Muller code of order $d < q-1$ is equal to $p_m-(d-1)q^{m-1}-p_{m-2}-q^{m-2}$.*

From Corollary 5 follows

Corollary 8 *Suppose Conjecture 3 holds, then the weight hierarchy of a projective q-ary Reed-Muller code of order $d < q$ is given by*

$$d_r = p_m - \sum_{i=j}^{m} \nu_i (p_{m-i} - p_{m-i-j}) + p_{m-2j},$$

where ν_i are such that $x_1^{\nu_1} x_2^{\nu_2} \dots x_{m+1}^{\nu_{m+1}}$ is the r-th (in lexicographical order) monomial of degree d in $m+1$ variables, and j is the smallest integer such that $\nu_j \neq 0$.

References

[1] M.Boguslavsky ' Del Pezzo surfaces and generalized weights', to appear in 'Problems of information transmission'.

[2] P.Delsarte, J.-M.Goethals and F.J.MacWilliams, 'On generalized Reed-Muller codes and their relatives,' Inform. and Control, vol. 16 (1974), pp. 423-442.

[3] T.Helleseth, T.Kløve and J.Mykkeltveit, 'The weight distribution of irreducible cyclic codes with block length $n_1 \left(\left(q^l - 1 \right) / N \right)$,' Discr. Math., vol. 18, 1977, pp.179-211.

[4] P. Heijnen and R. Pelikaan, 'Generalized Hamming weights for Reed-Muller codes,' preprint 1996.

[5] J.W.P. Hirschfeld, M.A.Tsfasman and S.G. Vlăduţ, 'The weight hierarchy of higher-dimensional Hermitian codes', IEEE Trans. Inform. Theory, v. 40, no. 1, January 1994, pp. 275-279.

[6] G. Lachaud, 'Number of points of plane sections and linear codes defined by forms on algebraic varieties,' in "Arithmetic, Geometry and Coding Theory", Walter de Gruyter, Berlin, 1996, pp. 77-104.

[7] F.J. MacWilliams and N.J.A. Sloane, *"The Theory of Error-correcting Codes,"* Elsevier, Amsterdam, 1977.

[8] D.Nogin, 'Generalized Hamming weights of codes on multidimensional quadrics'. Problems of information transmission, vol. 29, N 3, 1993, p. 21-30.

[9] D. Nogin 'Codes associated to Grassmanians,' in "Arithmetic, Geometry and Coding Theory," Walter de Gruyter, Berlin, 1996, pp. 145-154.

[10] W. Schmidt 'A lower bound for the number of solutions of equations over finite fields,' Journal of Number Theory, vol. 6 (1976), pp. 448-480.

[11] J.-P.Serre, ' Lettre à M. Tsfasman', in "Journées Arithmètiques de Luminy (1989)", Astèrisque 198-199-200 (1991), pp. 149-156.

[12] A.B. Sørensen, 'Rational points on hypersurfaces, Reed-Muller codes and algebraic-geometric codes,' Ph. D. Thesis, Aarhus, 1991.

[13] A.B. Sørensen, 'Projective Reed-Muller codes,' IEEE Trans. Inform. Theory, vol. 37 (1991), pp. 1567-1576.

[14] M.A. Tsfasman and S.G. Vlăduţ, *Algebraic - Geometric Codes.* Dordrecht: Kluwer Academic Publishers, 1991.

[15] M.A.Tsfasman and S.G. Vlăduţ, ' Geometric approach to higher weights'. IEEE Trans. Info. Theory, vol. 41, pp. 1564-1588, Nov. 1995.

[16] V.K. Wei, 'Generalized Hamming weights for linear codes'. IEEE Trans. Inform. Theory, vol.38, pp. 1125-1130, may 1992.

[17] V.K. Wei 'Generalized Hamming weights; Fundamental open problems in coding theory', in "Arithmetic, Geometry and Coding Theory," Walter de Gruyter, Berlin, 1996, pp.269-281.