An upper bound for the number of zeros of a system of homogeneous polynomials

Mrinmoy Datta

Department of Applied Mathematics and Computer Science
Technical University of Denmark
Copenhagen, Denmark

Joint work with Peter Beelen and Sudhir R. Ghorpade

Arithmetic, Geometry, Cryptography and Coding Theory - 2017

Notations:

The following notations will be used throughout the presentation.

- $\mathbb{F}_q$ = finite field with q elements for a prime power q.
- $R := \mathbb{F}_q[x_1, \ldots, x_m]$ and $R_{\leq d} := \{f \in R : \deg f \leq d\}$.
- $S := \mathbb{F}_q[x_0, \ldots, x_m]$ and $S_d := \{F \in S : F \text{ homogeneous } ; \deg F = d\}$.
- $\mathbb{A}^k(\mathbb{F}_q)$ = affine space of dimension k over $\mathbb{F}_q$.
- $\mathbb{P}^k(\mathbb{F}_q)$ = projective space of dimension k over $\mathbb{F}_q$.
- $p_k = |\mathbb{P}^k(\mathbb{F}_q)| = \begin{cases} 1 + q + \cdots + q^k & \text{if} \quad k \geq 0 \\ 0 & \text{if} \quad k < 0 \end{cases}$

Main question

Fix positive integers r, m, d with $d \leq q$.

Definitions

- For homogeneous polynomials $F_1, \ldots, F_r \in S$, define
  $\mathsf{V}(F_1, \ldots, F_r) := \{P \in \mathbb{P}^m(\mathbb{F}_q) : F_1(P) = \cdots = F_r(P) = 0\}$.
- $e_r(d, m) := \max \{|\mathsf{V}(F_1, \ldots, F_r)| : F_1, \ldots, F_r \in S_d \text{ linearly independent}\}$.

Question 1

Determine $e_r(d, m)$ for $r \leq \dim S_d = \binom{m+d}{d}$.

Connection with Projective Reed Muller Codes

Definition: Let $N = p_m$. Each point of $\mathbb{P}^m(\mathbb{F}_q)$ admits a unique representative in $\mathbb{F}_q^{m+1}$ in which the first nonzero coordinate is 1. Let $P_1, \ldots, P_N$ be an ordered listing of such representatives in $\mathbb{F}_q^{m+1}$of points of $\mathbb{P}^m(\mathbb{F}_q)$. The Projective Reed-Muller code of order d and length N is defined by

$$\mathrm{PRM}_q(d,m) := \{c_F := (F(P_1), \ldots, F(P_N)) : F \in S_d\}.$$

These codes were defined by Lachaud for $d \leq q$ and Sørensen for $d \leq m(q-1)$. If $d \leq q$, then the codeword c_F completely determines F, and thus

$$\dim \mathrm{PRM}_q(d,m) = \binom{m+d}{d}.$$

Moreover, if $d_r(d,m)$ denotes the r^{th} generalized Hamming weight or the r^{th} higher weight of $\mathrm{PRM}_q(d,m)$, then we see that

$$d_r(d,m) = N - e_r(d,m).$$

So Question 1 is equivalent to the determination of $d_r(d,m)$ when $d \leq q$.

An affine analogue

Fix positive integers r, m, d.

Definitions

- A polynomial $f \in R$ is said to be reduced if $\deg_{x_i} f \leq q-1$ for $i = 1, \ldots, m$.
- For $f_1, \ldots, f_r \in R$, $\mathsf{Z}(f_1, \ldots, f_r) := \{P \in \mathbb{A}^m(\mathbb{F}_q) : f_1(P) = \cdots = f_r(P) = 0\}$.
- $e_r^{\mathbb{A}}(d, m) :=$
  $\max\left\{|\mathsf{Z}(f_1, \ldots, f_r)| : f_1, \ldots, f_r \in R_{\leq d} \text{ linearly independent and reduced}\right\}$.

Question 2

Determine $e_r^{\mathbb{A}}(d, m)$ for $r \leq \dim R_{\leq d}$.

Answer to Question 2

Let $Q = \{0, 1, \ldots, q-1\}$. For $1 \leq r \leq \binom{m+d}{d}$, let $(\alpha_1, \ldots, \alpha_m)$ denote the r-th element in decreasing lexicographic order of the set

$$Q^m_{\leq d} = \{(\beta_1, \ldots, \beta_m) \in Q^m : \sum_{i=1}^{m} \beta_i \leq d\}.$$

Define

$$H_r(d, m) := \sum_{i=1}^{m} \alpha_i q^{m-i}.$$

Theorem (Heijnen-Pellikaan, 1998)

$e_r^{\mathbb{A}}(d, m) = H_r(d, m)$, *where* $1 \leq d \leq m(q-1)$ *and* $1 \leq r \leq \dim R_{\leq d}$.

Question 1: A brief history

- Small cases:
  (a) m=1: $e_r(d,1) = d - r + 1$, for $1 \leq r \leq d+1$.
  (b) d=1: $e_r(1,m) = p_{m-r}$ for $1 \leq r \leq m+1$.
  (c) r = 1: (Serre/ Sørensen) $e_1(d,m) = dq^{m-1} + p_{m-2}$.

Question 1: A brief history

- Small cases:
  (a) m=1: $e_r(d,1) = d - r + 1$, for $1 \leq r \leq d+1$.
  (b) d=1: $e_r(1,m) = p_{m-r}$ for $1 \leq r \leq m+1$.
  (c) r = 1: (Serre/ Sørensen) $e_1(d,m) = dq^{m-1} + p_{m-2}$.
- Boguslavsky, 1997 $e_2(d,m) = (d-1)q^{m-1} + q^{m-2} + p_{m-2}$, if $d < q-1$.

Question 1: A brief history

- Small cases:
  (a) m=1: $e_r(d,1) = d - r + 1$, for $1 \leq r \leq d+1$.
  (b) d=1: $e_r(1,m) = p_{m-r}$ for $1 \leq r \leq m+1$.
  (c) r = 1: (Serre/ Sørensen) $e_1(d,m) = dq^{m-1} + p_{m-2}$.
- Boguslavsky, 1997 $e_2(d,m) = (d-1)q^{m-1} + q^{m-2} + p_{m-2}$, if $d < q-1$.
- Zanella, 1998 For any integer t, define $\delta_t = \binom{t+2}{2}$. Let $r \leq \delta_m$ and k the unique integer $-1 \leq k < m$ such that $\delta_m - \delta_{k+1} < r \leq \delta_m - \delta_k$. Then

$$e_r(2,m) = Z_r := p_k + \lfloor q^{\epsilon-1} \rfloor, \quad \text{where } \epsilon = \delta_m - \delta_k - r.$$

Question 1: A brief history

- Small cases:
  (a) m=1: $e_r(d,1) = d - r + 1$, for $1 \leq r \leq d+1$.
  (b) d=1: $e_r(1,m) = p_{m-r}$ for $1 \leq r \leq m+1$.
  (c) r = 1: (Serre/ Sørensen) $e_1(d,m) = dq^{m-1} + p_{m-2}$.
- Boguslavsky, 1997 $e_2(d,m) = (d-1)q^{m-1} + q^{m-2} + p_{m-2}$, if $d < q-1$.
- Zanella, 1998 For any integer t, define $\delta_t = \binom{t+2}{2}$. Let $r \leq \delta_m$ and k the unique integer $-1 \leq k < m$ such that $\delta_m - \delta_{k+1} < r \leq \delta_m - \delta_k$. Then

$$e_r(2,m) = Z_r := p_k + \lfloor q^{\epsilon-1} \rfloor, \quad \text{where } \epsilon = \delta_m - \delta_k - r.$$

- Tsfasman-Boguslavsky conjecture (TBC), 1997 In a joint work with Sudhir Ghorpade, we have proved that the TBC is true for $r \leq m+1$ when $d < q-1$ and false, in general, for $r > m+1$.

Tsfasman-Boguslavsky Conjecture

Let $1 \leq r \leq K$. Let $(\nu_1, \ldots, \nu_{m+1})$ denote the r-th element in decreasing lexicographic order of the set

$$\mathscr{T}_{m,d} = \left\{ (\alpha_1, \ldots, a_{m+1}) \in \mathbb{N}_0^{m+1} : \sum_{i=1}^{m+1} \alpha_i = d \right\}.$$

Define

$$T_r(d,m) := p_{m-2j} + \sum_{i=j}^{m} \nu_i (p_{m-i} - p_{m-i-j}) \quad \text{where } j := \min\{i : \nu_i \neq 0\}.$$

Conjecture (Tsfasman Boguslavsky, 1997)

For $1 \leq d < q-1$ and $1 \leq r \leq \binom{m+d}{d}$ we have, $e_r(d,m) = T_r(d,m)$.

A conjecture

Conjecture 1 (with Sudhir Ghorpade, 2016)

For $1 \leq d \leq q-1$, we have $e_r(d,m) = C_r(d,m) := H_r(d-1,m) + p_{m-1}$ for $1 \leq r \leq \binom{m+d-1}{m}$.

Observation: $\boxed{e_r(d,m) \geq C_r(d,m).}$

Proof: For $1 \leq r \leq \binom{m+d-1}{d-1}$ let $f_1, \ldots, f_r \in R_{\leq d-1}$ be linearly independent polynomials such that

$$|\mathsf{Z}(f_1, \ldots, f_r)| = H_r(d-1,m).$$

The existence of such a family is assured due to Heijnen-Pellikaan Theorem. Let $F_1, \ldots, F_r \in S_d$ be the set of polynomials obtained by homogenizing $f_1, \ldots, f_r$ to degree d. It is not hard to check that $F_1, \ldots, F_r$ are linearly independent and $|\mathsf{V}(F_1, \ldots, F_r)| = C_r(d,m)$.

Remark: Note that the conjecture is true for $d = 1$ and $d = 2$.

Contributions..

- Theorem 1 (with Sudhir Ghorpade, 2016)
  Conjecture 1 is true for $1 \leq r \leq m+1$, if $d < q-1$.
- Theorem 2 (with Peter Beelen and Sudhir Ghorpade, to appear)
  Conjecture 1 is true for $1 \leq r \leq \binom{m+2}{2}$, if $2 < d \leq q-1$.
- Theorem 3 (with Peter Beelen and Sudhir Ghorpade, to appear)
  Let $q \geq 3$[1] and $d = q$. Then,

$$e_r(d,m) = \begin{cases} q^{m-1} + p_{m-r-1} & \text{if } \ 1 \leq r \leq m \\ (q-1)q^{m-1} + p_{m-2} & \text{if } \ r = m+1 \end{cases}$$

Remark Theorem 2 shows that Conjecture 1 is true for $d = 3$.

[1] The case $d = q = 2$ is already taken care of by Zanella's theorem.

Sketch of proof of Theorem 2

The main goal is to prove that,

$$e_r(d,m) \leq C_r(d,m) = H_r(d-1,m) + p_{m-1}. \quad \text{for} \quad 1 \leq r \leq \binom{m+2}{2}. \tag{1}$$

Let $F_1, \ldots, F_r \in S_d$ be linearly independent. Let $G = \gcd(F_1, \ldots, F_r)$ and $c := \deg G$. Thus $F_i = G.F_i'$ and $F_1', \ldots, F_r'$ are coprime. We proceed by induction on $m + d$.

Suppose $c > 0$:

- If G has a linear factor, then it is easy to check that (1) holds.
- If G has no linear factors, then we use an upperbound, due to Homma and Kim, of the number of $\mathbb{F}_q$-rational points on a hypersurface having no linear component d along with the induction hypothesis to deduce (1).

We may thus assume that $c = 0$, i. e. $F_1, \ldots, F_r$ are coprime.

Sketch of proof of Theorem 2 (contd)

Recall $F_1, \ldots, F_r \in S_d$, $1 \leq r \leq \binom{m+2}{2}$ and $\gcd(F_1, \ldots, F_r) = 1$. Let W be the $\mathbb{F}_q$ linear subspace generated by $F_1, \ldots, F_r$.

Definition: The t- invariant of W, denoted t_W, is defined to be the highest dimension of a subspace of W consisting of polynomials that have a common linear factor.

Choose a linear polynomial H that corresponds to t_W. Write,

$$|\mathrm{V}(F_1, \ldots, F_r)| = |\mathrm{V}(F_1, \ldots, F_r) \cap \Pi| + |\mathrm{V}(F_1, \ldots, F_r) \cap \Pi^C|,$$

where $\Pi = V(H)$.

- Note that
  - $|\mathrm{V}(F_1, \ldots, F_r) \cap \Pi| \leq e_{r-t_W}(d, m-1)$ (can be estimated by induction).
  - $|\mathrm{V}(F_1, \ldots, F_r) \cap \Pi^C| \leq H_{t_W}(d-1, m)$.
- The case where t_W is very small is dealt with a lemma of Zanella.
- The case where t_W is large can be solved using estimates involving the quantites $H_r(d, m)$.
- The rest of the cases are dealt using induction hypothesis and a variant of a Theorem by Lachaud and Rolland.

Remarks on Theorem 3

Theorem 3 (with Peter Beelen and Sudhir Ghorpade, 2016)
Let $q \geq 3$ and $d = q$. Then,

$$e_r(d,m) = \begin{cases} q^{m-1} + p_{m-r-1} & \text{if } 1 \leq r \leq m \\ (q-1)q^{m-1} + p_{m-2} & \text{if } r = m+1 \end{cases}$$

Remarks:

- For $1 \leq r \leq m$, the family of polynomials $F_1, \ldots, F_r$, given by

  $$F_i = x_i^q - x_0^{q-1} x_i$$

  has $q^{m-1} + p_{m-r-1}$ common zeroes in $\mathbb{P}^m(\mathbb{F}_q)$, which shows that $e_r(m,q) \geq q^{m-1} + p_{m-r-1}$.
- For $r = m+1$, the ingredients of the proof of the inequality $e_r(d,m) \leq C_r(d,m)$ are similar to that of Theorem 2.

Work in progress

Notation:

- r, m, d positive integers.
- $Q = \{0, 1, \ldots, q-1\}$.
- $Q^m_{\leq d} = \{(\beta_1, \ldots, \beta_m) \in Q^m : \sum \beta_i \leq d\}$.

Theorem (With Peter Beelen and Sudhir Ghorpade)

Let $1 \leq r \leq q-1$. Let $(\alpha_1, \ldots, \alpha_m) \in Q^m$ be the r-th element of $Q^m_{\leq d}$ in descending lexicographic order. Then

$$e_r(d, m) \leq \sum_{i=1}^{m} \alpha_i p_{m-i}.$$

The above Theorem gives us the exact value of $e_r(d, m)$ for several values of $r \geq \binom{m+2}{2}$, but in general this bound is not tight.

Thank you!