Old and New Conjectures on the Number of Points of Algebraic Sets over Finite Fields

Sudhir R. Ghorpade

Department of Mathematics
Indian Institute of Technology Bombay
Powai, Mumbai 400076, India
srg@math.iitb.ac.in
http://www.math.iitb.ac.in/∼srg/

Number Theory and Geometry,
Alexey Zykin Memorial Conference
Independent University of Moscow and all over the world
June 19, 2020

Dedicatory

This talk is dedicated to the memory of
Alexey Zykin (13 June 1984 – 23 April 2017).

[Source: Google Images/Gmail Profile pic of Alexey.]

Algebraic Varieties over Finite Fields

Let X be an (irreducible) projective algebraic variety in $\mathbb{P}^m$ defined over $\mathbb{F}_q$ of dimension n. Let $p_n := |\mathbb{P}^n(\mathbb{F}_q)| = q^n + q^{n-1} + \cdots + 1$.

Algebraic Varieties over Finite Fields

Let X be an (irreducible) projective algebraic variety in $\mathbb{P}^m$ defined over $\mathbb{F}_q$ of dimension n. Let $p_n := |\mathbb{P}^n(\mathbb{F}_q)| = q^n + q^{n-1} + \cdots + 1$.

- Lang-Weil Inequality (1954). If X has degree d, then

$$\Big| |X(\mathbb{F}_q)| - p_n \Big| \leq (d-1)(d-2)q^{n-(1/2)} + Cq^{n-1},$$

where C is a constant depending only on m, n and d.

Algebraic Varieties over Finite Fields

Let X be an (irreducible) projective algebraic variety in $\mathbb{P}^m$ defined over $\mathbb{F}_q$ of dimension n. Let $p_n := |\mathbb{P}^n(\mathbb{F}_q)| = q^n + q^{n-1} + \cdots + 1$.

- Lang-Weil Inequality (1954). If X has degree d, then

$$\left| |X(\mathbb{F}_q)| - p_n \right| \leq (d-1)(d-2)q^{n-(1/2)} + Cq^{n-1},$$

  where C is a constant depending only on m, n and d.

- Deligne's Inequality (1973). If X is a nonsingular complete intersection, then

$$\left| |X(\mathbb{F}_q)| - p_n \right| \leq b_n' \, q^{n/2}.$$

  where $b_n' = b_n - \epsilon_n$ is its primitive nth Betti number of X (where $\epsilon_n = 1$ if n is even and $\epsilon_n = 0$ if n is odd).

Algebraic Varieties over Finite Fields

Let X be an (irreducible) projective algebraic variety in $\mathbb{P}^m$ defined over $\mathbb{F}_q$ of dimension n. Let $p_n := |\mathbb{P}^n(\mathbb{F}_q)| = q^n + q^{n-1} + \cdots + 1$.

- Lang-Weil Inequality (1954). If X has degree d, then
$$\Big| |X(\mathbb{F}_q)| - p_n \Big| \leq (d-1)(d-2)q^{n-(1/2)} + Cq^{n-1},$$
where C is a constant depending only on m, n and d.
- Deligne's Inequality (1973). If X is a nonsingular complete intersection, then
$$\Big| |X(\mathbb{F}_q)| - p_n \Big| \leq b'_n \, q^{n/2}.$$
where $b'_n = b_n - \epsilon_n$ is its primitive nth Betti number of X (where $\epsilon_n = 1$ if n is even and $\epsilon_n = 0$ if n is odd).

Remark: If X has multidegree $\mathbf{d} = (d_1, \ldots, d_r)$, then b'_n equals
$$(-1)^{n+1}(n+1) + \sum_{c=r}^{m} (-1)^{m+c} \binom{m+1}{c+1} \sum_{\substack{\nu_1+\cdots+\nu_r=c \\ \nu_i \geq 1 \ \forall i}} d_1^{\nu_1} \cdots d_r^{\nu_r}$$

Extensions and Generalizations

Some extensions and improvements of these results are known. Namely, an effective version of Lang-Weil inequality with an explicit bound on the constant C appearing therein, and an extension of Deligne's inequality for possibly singular complete intersections are known. [cf. G-Lachaud (*MMJ*, 2002)]. However, all these results assume that X is irreducible.

Extensions and Generalizations

Some extensions and improvements of these results are known. Namely, an effective version of Lang-Weil inequality with an explicit bound on the constant C appearing therein, and an extension of Deligne's inequality for possibly singular complete intersections are known. [cf. G-Lachaud (*MMJ*, 2002)]. However, all these results assume that X is irreducible.

Question: What is X is possibly reducible? In other words, do we have good estimates for $|X(\mathbb{F}_q)|$ when X is a projective algebraic set, or an affine algebraic set?

Extensions and Generalizations

Some extensions and improvements of these results are known. Namely, an effective version of Lang-Weil inequality with an explicit bound on the constant C appearing therein, and an extension of Deligne's inequality for possibly singular complete intersections are known. [cf. G-Lachaud (*MMJ*, 2002)]. However, all these results assume that X is irreducible.

Question: What is X is possibly reducible? In other words, do we have good estimates for $|X(\mathbb{F}_q)|$ when X is a projective algebraic set, or an affine algebraic set?

Simplest Case: Ore's Inequallity (1933). If X is an affine hypersurface in $\mathbb{A}^m$ defined by a polynomial $f(x_1, \dots, x_m)$with coefficients in $\mathbb{F}_q$, then it is not difficult to show that

$$|X(\mathbb{F}_q)| \leq dq^{m-1}.$$

The bound dq^{m-1} is trivial if $d \geq q$ and it is attained if $d < q$, e.g., we can take $f(x_1, \dots, x_m) = (x_1 - a_1) \cdots (x_1 - a_d)$, where $a_1, \dots, a_d$ are distinct elements of $\mathbb{F}_q$.

The Case of a Projective Hypersurface

Let $F \in \mathbb{F}_q[x_0, x_1, \dots, x_m]$ be a nonzero homogeneous polynomial of degree d and let $X = V(F)$ be the corresponding hypersurface.

Natural Guess: $|X(\mathbb{F}_q)| \le dp_{m-1}$.

The Case of a Projective Hypersurface

Let $F \in \mathbb{F}_q[x_0, x_1, \dots, x_m]$ be a nonzero homogeneous polynomial of degree d and let $X = V(F)$ be the corresponding hypersurface.

Natural Guess: $|X(\mathbb{F}_q)| \le dp_{m-1}$.

Heuristics: Project X onto $\mathbb{P}^{m-1}$. There are p_{m-1} points in $\mathbb{P}^{m-1}$ and above each of them, there are at most d points on X.

The Case of a Projective Hypersurface

Let $F \in \mathbb{F}_q[x_0, x_1, \dots, x_m]$ be a nonzero homogeneous polynomial of degree d and let $X = V(F)$ be the corresponding hypersurface.

Natural Guess: $|X(\mathbb{F}_q)| \le dp_{m-1}$.

Heuristics: Project X onto $\mathbb{P}^{m-1}$. There are p_{m-1} points in $\mathbb{P}^{m-1}$ and above each of them, there are at most d points on X.

Note that if $d > q$, then $dp_{m-1} \ge (q+1)p_{m-1} \ge p_m$ and so the bound is interesting only when $d \le q$. In this case, we may be tempted to assume that the bound is optimum and try the analogue of the affine example, namely, the homogeneous polynomial $F(x_0, x_1, \dots, x_m) = (x_1 - a_1 x_0) \cdots (x_1 - a_d x_0)$, where $a_1, \dots, a_d$ are distinct elements of $\mathbb{F}_q$. In this case,

$$|X(\mathbb{F}_q)| = dq^{m-1} + p_{m-2}.$$

Note that the RHS is $< dp_{m-1}$ if $d > 1$.

A Conjecture of Tsfasman

M. A. Tsfasman conjectured in the late 1980's that

> *If* $0 \neq F \in \mathbb{F}_q[x_0, x_1, \ldots, x_m]$ *is homogeneous of degree* $d \leq q$, *then* $|V(F)| \leq dq^{m-1} + p_{m-2}$. *Consequently,* $\max\{|V(F)| : 0 \neq F \in \mathbb{F}_q[x_0, \ldots, x_m]_d\} = dq^{m-1} + p_{m-2}$.

A Conjecture of Tsfasman

M. A. Tsfasman conjectured in the late 1980's that

> *If* $0 \neq F \in \mathbb{F}_q[x_0, x_1, \ldots, x_m]$ *is homogeneous of degree* $d \leq q$*, then* $|V(F)| \leq dq^{m-1} + p_{m-2}$. *Consequently,* $\max\{|V(F)| : 0 \neq F \in \mathbb{F}_q[x_0, \ldots, x_m]_d\} = dq^{m-1} + p_{m-2}$.

This was soon proved by J.-P. Serre (*Astérisque*, 1991) and independently by A. B. Sørensen (*IEEE Trans. Inform. Theory*, 1991). Serre's proof is quite beautiful and proceeds as follows.

- Induct on m. The case $m = 1$ is clear. Suppose $m > 1$ and the result holds for smaller values of m.
- Let $G_1, \ldots, G_t$ be distinct (homogeneous) linear factors of F, and let $L_i = V(G_i)$ be the corresponding hyperplanes and

$$L = \bigcup_{i=1}^{t} L_i.$$

- Note that $t \leq d$ and $L \subseteq V(F)$. We now divide the proof in two cases according as $L = V(F)$ and $L \neq V(F)$.

Serre's proof of $|V(F)| \le dq^{m-1} + p_{m-2}$

Case 1. $L = V(F)$.
In this case we induct on t. The case $t = 0$ is trivial, whereas if $t = 1$, then

$$|L| = |L_1| = p_{m-1} = q^{m-1} + p_{m-2} \le dq^{m-1} + p_{m-2}.$$

Suppose $t > 1$. Then

$$\begin{aligned}
\left| \bigcup_{i=1}^{t} L_i \right| &= \left| \bigcup_{i=1}^{t-1} L_i \right| + |L_t| - \left| \bigcup_{i=1}^{t-1} L_i \cap L_t \right| \\
&\le \left[(t-1)q^{m-1} + p_{m-2}\right] + p_{m-1} - p_{m-2} \\
&= tq^{m-1} + p_{m-2} \\
&\le dq^{m-1} + p_{m-2},
\end{aligned}$$

as desired.

Serre's proof of $|V(F)| \le dq^{m-1} + p_{m-2}$ Contd.

Case 2. $L \ne V(F)$.

In this case, there exists $P \in V(F)$ such that $P \notin L$.

- If $H \in \widehat{\mathbb{P}}^m$ (i.e., H is a hyperplane in $\mathbb{P}^m$) with $P \in H$, then $F|_H \ne 0$ and hence by induction hypothesis,

$$\Big| V(F) \cap H \Big| \le dq^{m-2} + p_{m-3}.$$

- Consider the incidence set

$$\mathcal{I} = \Big\{ (P', H) : P' \in V(F) \setminus \{P\},\ H \in \widehat{\mathbb{P}}^m \text{ with } P, P' \in H \Big\}$$

  and count it in two different ways as follows.

- $|\mathcal{I}| = (|V(F)| - 1)\, p_{m-2}$
- $|\mathcal{I}| = p_{m-1}\, (|V(F) \cap H| - 1)$.

Consequently, $(|V(F)| - 1)\, p_{m-2} \le p_{m-1}\left(dq^{m-2} + p_{m-3} - 1\right)$.

Serre's proof of $|V(F)| \le dq^{m-1} + p_{m-2}$ Contd.

Since $(|V(F)| - 1)\, p_{m-2} \le p_{m-1}\left(dq^{m-2} + p_{m-3} - 1\right)$,

$$\begin{aligned}
|V(F)| &\le \frac{p_{m-2} + p_{m-1}\left(dq^{m-2} + p_{m-3} - 1\right)}{p_{m-2}} \\
&= \frac{-q^{m-1} + dq^{m-2}p_{m-1} + p_{m-1}p_{m-3}}{p_{m-2}} \\
&= \frac{-q^{m-1} + dq^{m-2}(qp_{m-2} + 1) + (qp_{m-2} + 1)\frac{(p_{m-2} - 1)}{q}}{p_{m-2}} \\
&= dq^{m-1} + p_{m-2} - \frac{(q+1-d)q^{m-2}}{p_{m-2}} \\
&< dq^{m-1} + p_{m-2}. \qquad \square
\end{aligned}$$

Remark: The above proof shows that the bound is attained only when $V(F)$ is a union of hyperplanes; in fact, a union of d hyperplanes with an $(m-2)$-dimensional projective linear space in common.

Several homogeneous polynomials in several variables

It turns out that one might hope to find an extension of Serre's Theorem for the number of common zeros in $\mathbb{P}^m(\mathbb{F}_q)$ of several homogeneous polynomials in $m+1$ variables, provided they all have the same degree d. It is also natural to assume that the polynomials are linearly independent. This forces, of course, that the number of polynomials is $\le \dim_{\mathbb{F}_q} \mathbb{F}_q[x_0, x_1, \dots, x_m]_d = \binom{d+m}{d}$.

Several homogeneous polynomials in several variables

It turns out that one might hope to find an extension of Serre's Theorem for the number of common zeros in $\mathbb{P}^m(\mathbb{F}_q)$ of several homogeneous polynomials in $m+1$ variables, provided they all have the same degree d. It is also natural to assume that the polynomials are linearly independent. This forces, of course, that the number of polynomials is $\le \dim_{\mathbb{F}_q} \mathbb{F}_q[x_0, x_1, \dots, x_m]_d = \binom{d+m}{d}$.

Conjecture (Tsfasman-Boguslavsky)

Let $F_1, \dots, F_r \in \mathbb{F}_q[x_0, x_1, \dots, x_m]$ be linearly indep. homogeneous polynomials of degree $d < q-1$ and $V = V(F_1, \dots, F_r)$ be the set of their common zeros $\mathbb{P}^m(\mathbb{F}_q)$. Let $(\nu_1, \ \dots, \ \nu_{m+1})$ be the r-th tuple in the list of exponent vectors of monomials of degree d in $m+1$ variables, ordered lexicographically in descending order, and let $j = \min\{i : 1 \le i \le m+1 \textit{ and } \nu_i \ne 0\}$. Then

$$|V(\mathbb{F}_q)| \le p_{m-2j} + \sum_{i=j}^{m} \nu_i (p_{m-i} - p_{m-i-j}).$$

Tsfasman-Boguslavsky Conjecture (TBC)

The conjecture, in fact, not only gives an upper bound on $\#V$, but claims that this is the best bound possible. In other words,

$$e_r(d,m)$$
$$:= \max\{|V(F_1,\dots,F_r)| : F_1,\dots,F_r \in \mathbb{F}_q[x_0,x_1,\dots,x_m]_d \text{ lin. indep.}\}$$
$$= p_{m-2j} + \sum_{i=j}^{m} \nu_i(p_{m-i} - p_{m-i-j}) \quad \text{for } d < q-1,$$

where $(\nu_1, \dots, \nu_{m+1})$ and j are as above.

Example: Clearly, $(d, 0, 0, \dots, 0)$ is the largest $(m+1)$-tuple of exponent vectors of monomials in $(m+1)$-variables of degree d. Thus if $r = 1$, then $\nu_1 = d$, $\nu_i = 0$ for $i > 1$ and $j = 1$ so that

$$e_1(d,m) = p_{m-2} + d(p_{m-1} - p_{m-2}),$$

exactly as in Serre's bound. In case $r = 2$ and $d > 1$, then $(d-1,1,0,\dots,0)$ is the second tuple and the bound becomes

$$e_2(d,m) = (d-1)q^{m-1} + q^{m-2} + p_{m-2}.$$

Another Estimate for Projective Algebraic Sets

Couvreur (*PAMS*, 2016) settled the so called Ghorpade-Lachaud Conjecture, which can be viewed as a counterpart of the TBC.

Theorem (Couvreur)

Let X be a nondegenerate projective algebraic set in $\mathbb{P}^m$ defined over $\mathbb{F}_q$. Suppose the irreducible components of X have dimensions $n_1, \dots, n_t$ and degrees $\delta_1, \dots, \delta_t$, respectively. If $n_i < m$ for all $i = 1, \dots, t$, and if $n := \max\{n_1, \dots, n_t\}$, then

$$|X(\mathbb{F}_q)| \le p_{2n-m} + \sum_{i=1}^{t} \delta_i \left(p_{n_i} - p_{2n_i - m}\right) \qquad (1)$$

In particular, if X is equidimensional of dim n and degree δ, then

$$|X(\mathbb{F}_q)| \le \delta p_n - (\delta - 1) p_{2n-m} = \delta(p_n - p_{2n-m}) + p_{2n-m}. \qquad (2)$$

Remark: (2) reduces to Serre's inequality if $\mathrm{codim} X = m - n = 1$.

Comparision with Couvreur's theorem

In general, the hypothesis of TBC is amenable to an easy verification. In the equidimensional case, the Couvreur bound, say $C_r(m)$, is often better than the Tsfasman-Boguslavsky bound, say $T_r(d,m)$. Suppose $X \subseteq \mathbb{P}^m$ is defined by the vanishing of r linearly independent homogeneous polynomials in $m+1$ variables, each of the same degree d, and $n = \dim X = m - r$ so that X is a complete intersection of degree $\delta = d^r$. Assume, for simplicity, that $n \geq 0$, i.e., $r \leq m$, and that $d > 1$, $\delta \leq q+1$. Then

$$C_r(m) \leq T_r(d,m).$$

On the other hand, in the non-equidimensional case, the Tsfasman-Boguslavsky bound can be better than the Couvreur bound. For example, if $r \leq m$ and $Q_1, \dots, Q_r$ are quadrics defined by $Q_i = x_0 x_i$ for $i = 1, \dots, r$, and if $V = V(Q_1, \dots, Q_r)$, then

$$|V| = T_r(2,m) = p_{m-1} + q^{m-r} < p_{m-1} + q^{m-r} + \cdots + q^{m-2r+1} = C_r(m).$$

Thus the two bounds complement each other and neither implies the other.

Boguslavsky's Theorem

Tsfasman-Boguslavsky Conjecture, which dates back to mid to late 1990's is still open, in general. After Serre bound, the next significant result was obtained by M. Boguslavsky (*Finite Fields Appl.*, 1997) where he settled the $r = 2$ case.

Theorem (Boguslavsky, 1997)

Assume that $1 < d < q - 1$. *Then*

$$e_2(d, m) = (d-1)q^{m-1} + q^{m-2} + p_{m-2}.$$

The proof is quite intricate. It uses the Serre bound, reduction to certain complete intersections, and the use of the following basic inequality essentially due to G. Lachaud.

> *If V is an equidimensional projective variety in $\mathbb{P}^m$ defined over $\mathbb{F}_q$ of dimension n and degree d, then*
> $$\#V(\mathbb{F}_q) \leq dp_n.$$

Affine Case

It turns out that an affine analogue of Tsfasman-Boguslavsky Conjecture is known, in general. This corresponds of course to the maximum number of zeros that a system of r polynomial equations of degree d in $\mathbb{F}_q[x_1, \ldots, x_m]$ can have. The answer is given by:

Theorem (Heijnen-Pelikaan, 1998)

Let $f_1, \ldots, f_r$ be linearly independent polynomials of degree $d > 1$ in $\mathbb{F}_q[x_1, \ldots, x_m]$. Then the maximum number of common zeros in $\mathbb{A}^m(\mathbb{F}_q)$ that $f_1, \ldots, f_r$ can have is given by

$$H_r(d, m) := q^m - \left(1 + \sum_{i=1}^{m} \alpha_{m-i+1} q^{i-1}\right),$$

where $(\alpha_1, \ldots, \alpha_m)$ is the r^{th} tuple among the m-tuples $(\beta_1, \ldots, \beta_m)$ with coordinates from $\{0, 1, \ldots, q-1\}$ satisfying $\beta_1 + \cdots + \beta_m \geq m(q-1) - d$, where the tuples are arranged lexicographically in ascending order.

Illustration of Heijnen-Pelikaan Theorem

As a simple illustration of the Heijnen-Pelikaan Theorem, consider the case $r = 1$. Then one can see that the first m-tuple satisfying the conditions of the theorem is

$$(q-1-d,\ q-1,\ q-1,\ \ldots, q-1).$$

Hence in this case

$$\begin{aligned} H_r(d,m) &= q^m - \left(1 + \sum_{i=1}^{m} \alpha_{m-i+1} q^{i-1}\right) \\ &= q^m - \left(1 + (q-1-d)q^{m-1} + \sum_{i=1}^{m-1} (q-1)q^{i-1}\right) \\ &= dq^{m-1}, \end{aligned}$$

as is to be expected. The proof of the theorem, in general, is quite involved and uses combinatorial results such as Kruskal-Katona Theorem.

Alternative Description of Heijnen-Pelikaan Theorem

- It is not difficult to see that

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

  where $(\beta_1, \dots, \beta_m)$ is the rth element in descending lexicographic order among all m-tuples $(\gamma_1, \dots, \gamma_m)$ of nonnegative integers satisfying $\gamma_1 + \cdots + \gamma_m \le d$.

- Let $\mathbb{F}_q[x_1, \dots, x_m]_{\le d}$ denote the $\mathbb{F}_q$-vector space of polynomials in m variables $x_1, \dots, x_m$ of degree $\le d$. Define

$$e_r^{\mathbb{A}}(d,m) := \max\left\{|Z(f_1, \dots, f_r)| : f_1, \dots, f_r \in \mathbb{F}_q[x_1, \dots, x_m]_{\le d} \text{ lin indep}\right\}$$

Theorem (Heijnen-Pelikaan, 1998; Beelen-Datta, 2018)

For $1 \le d < q$, $m \ge 1$, and $1 \le r \le \binom{m+d}{d}$,

$$e_r^{\mathbb{A}}(d,m) := H_r(d,m).$$

Another Geometric Viewpoint

Finding the maximum number of common zeros of r linearly independent homogeneous polynomials of degree d in $m+1$ variables over $\mathbb{F}_q$ corresponds to finding the maximum number of $\mathbb{F}_q$-rational points in sections of the Veronese variety

$$\mathscr{V}_{d,m} := \nu_d(\mathbb{P}^m) \hookrightarrow \mathbb{P}^{\binom{m+d}{d}-1}$$

by (projective) linear subspaces of codimension r.

Another Geometric Viewpoint

Finding the maximum number of common zeros of r linearly independent homogeneous polynomials of degree d in $m+1$ variables over $\mathbb{F}_q$ corresponds to finding the maximum number of $\mathbb{F}_q$-rational points in sections of the Veronese variety

$$\mathscr{V}_{d,m} := \nu_d(\mathbb{P}^m) \hookrightarrow \mathbb{P}^{\binom{m+d}{d}-1}$$

by (projective) linear subspaces of codimension r. We remark that one can also consider linear sections of the Grassmann variety

$$G_{\ell,m} := \{\ell\text{-dimensional subspaces of } \mathbb{F}_q^m\} \hookrightarrow \mathbb{P}^{\binom{m}{\ell}-1}.$$

Another Geometric Viewpoint

Finding the maximum number of common zeros of r linearly independent homogeneous polynomials of degree d in $m+1$ variables over $\mathbb{F}_q$ corresponds to finding the maximum number of $\mathbb{F}_q$-rational points in sections of the Veronese variety

$$\mathscr{V}_{d,m} := \nu_d(\mathbb{P}^m) \hookrightarrow \mathbb{P}^{\binom{m+d}{d}-1}$$

by (projective) linear subspaces of codimension r. We remark that one can also consider linear sections of the Grassmann variety

$$G_{\ell,m} := \{\ell\text{-dimensional subspaces of } \mathbb{F}_q^m\} \hookrightarrow \mathbb{P}^{\binom{m}{\ell}-1}.$$

or related projective algebraic varieties such as Schubert varieties, determinantal varieties, etc. There are many interesting results and questions in these directions. That will probably need at least one more talk. But Those interested may see some of my papers available below and the references therein:

http://www.math.iitb.ac.in/∼srg/Papers.html

Progress on TBC

The Tsfasman-Boguslavsky Conjecture, which predicts the exact value of $e_r(d, m)$ for $d < q$, was open for almost two decades. It was settled about 5 years ago in the following sense.

Theorem (Joint work with Mrinmoy Datta, *Moscow Math J., 2015*)

The Tsfasman-Boguslavsky Conjecture is true if $d = 2$ *and* $r \le m + 1$, *but it is false, in general. More precisely, if* $d = 2$ *and* $m > 2$, *then it is false for at least* $\binom{m-1}{2}$ *values of positive integers* r *with* $m + 1 < r \le \binom{m+2}{2}$.

Progress on TBC

The Tsfasman-Boguslavsky Conjecture, which predicts the exact value of $e_r(d, m)$ for $d < q$, was open for almost two decades. It was settled about 5 years ago in the following sense.

Theorem (Joint work with Mrinmoy Datta, *Moscow Math J., 2015*)

The Tsfasman-Boguslavsky Conjecture is true if $d = 2$ and $r \leq m + 1$, but it is false, in general. More precisely, if $d = 2$ and $m > 2$, then it is false for at least $\binom{m-1}{2}$ values of positive integers r with $m + 1 < r \leq \binom{m+2}{2}$.

Theorem (Joint work with Mrinmoy Datta, *Proc. AMS, 2017*)

The Tsfasman-Boguslavsky Conjecture is true for any $r \leq m + 1$ and $d < q - 1$.

The proof of the last theorem uses Serre's inequality, but not Boguslavsky's Theorem, and so we obtain Boguslavsky's Theorem as a corollary.

Remarks on the proof of Theorem 1:

The key idea is to use the following:

Theorem [Zanella, 1998] For any integer t, define $\delta_t = \binom{t+2}{2}$. Let $r \leq \delta_m$ and k the unique integer with $-1 \leq k < m$ such that $\delta_m - \delta_{k+1} < r \leq \delta_m - \delta_k$. Then for any linear subspace L_r of codimension r in $\mathbb{P}^{\delta_m - 1}$,

$$|\mathscr{V}_{m,2} \cap L_r| \leq Z_r := p_k + \lfloor q^{\epsilon - 1} \rfloor, \quad \text{where } \epsilon = \delta_m - \delta_k - r.$$

To show that the TBC is false, in general for $d = 2$ and $r > m+1$, it suffices to show that $Z_r < T_r(2, m)$. This is done for at least $\binom{m-1}{2}$ values for r with $m+1 < r \leq \delta_m$, provided $m > 2$.

To show that the [TBC is true when $d = 2$ and $r \leq m+1$, one has to show that $Z_r = T_r(2, m)$ in this case and give explicit examples where the bound is attained. The latter is done as follows.

- For $1 \leq r \leq m$, the bound is attained if we take $F_i = x_0 x_i$ for $i = 1, 2, \ldots, r$. For $r = m+1$, the bound is attained if we take

$$F_i = x_0 x_i \quad \text{for } i = 1, 2, \ldots, m \quad \text{and} \quad F_{m+1} = x_0^2.$$

Remarks on the proof of Theorem 2:

Theorem

For $1 \le r \le m+1$ and $1 < d < q-1$, we have

$$e_r(d,m) = (d-1)q^{m-1} + p_{m-2} + \lfloor q^{m-r} \rfloor.$$

The main ingredients in the proof are as follows:

- Serre's inequality
- Theorem of Heijnen-Pellikaan
- A basic bound due to Lachaud for projective algebraic sets
- Characterization of a "coprime close" family of polynomials
- Case by case analysis
- Explicit constructions of maximal families when $r \le m+1$.

What's next?

Theorems 1 and 2 settle in a way the Tsfasman-Boguslavsky conjecture. However, the question about the determination of $e_r(d,m)$ still remains open in cases not covered by the earlier results. Generally speaking, the results obtained thus far do not yield the exact values of

- $e_r(d,m)$ whenever $m+1 < r \leq \binom{m+d}{d} - d - 1$ and $2 < d < q-1$.
- $e_r(d,m)$ whenever $1 < r \leq \binom{m+d}{d}$ and $d \geq q-1$.

Conjecture (The "Incomplete Conjecture")

For $1 < d < q$ and $r \leq \binom{m+d-1}{d-1}$,

$$e_r(d,m) = H_r(d-1,m) + p_{m-1}.$$

Theorem (Joint with P. Beelen and M. Datta, *Proc. AMS*, 2018)

The above conjecture is true for $1 < d < q$ and $r \leq \binom{m+2}{2}$.

Remarks on the proof of Theorem 3

Theorem (Explicit form of the last theorem)

For $1 < d < q$ *and* $r \leq \binom{m+2}{2}$.

$$e_r(d, m) = (d-2)q^{m-1} + p_{m-2} + \lfloor q^{m-i} \rfloor + \lfloor q^{m-j} \rfloor,$$

where i, j *are unique integers with* $1 \leq i \leq j \leq m+1$ *and* $r = (i-1)m - \binom{i-1}{2} + j$.

The main ingredients in the proof are as follows:

- Serre's inequality
- Theorem of Heijnen-Pellikaan
- Theorem of Zanella
- A variant of Bèzout's theorem by Lachaud and Rolland (2015)
- Inequality of Homma and Kim (2013) about the maximum number of points on hypersurfaces without a $\mathbb{F}_q$-linear component

More Recent Results (Joint with P. Beelen and M. Datta)

Completing the incomplete: A starting point is the binomial identity for positive integers d, m.

$$\binom{m+d}{d} = \binom{m+d-1}{d-1} + \binom{m+d-2}{d-1} + \cdots + \binom{d-1}{d-1}$$

More Recent Results (Joint with P. Beelen and M. Datta)

Completing the incomplete: A starting point is the binomial identity for positive integers d, m.

$$\binom{m+d}{d} = \binom{m+d-1}{d-1} + \binom{m+d-2}{d-1} + \cdots + \binom{d-1}{d-1}$$

and also that for any $1 \le r < \binom{m+d}{d}$, there are unique integers i, j such that

$$r = \binom{m+d-1}{d-1} + \cdots + \binom{m+d-i}{d-1} + j,$$

where

$$0 \le i \le m, \quad \text{and} \quad 0 \le j < \binom{m+d-i-1}{d-1}.$$

By convention, $i := m$ and $j := \binom{m+d-i-1}{d-1} = 1$ when $r = \binom{m+d}{d}$.

More Recent Results (Contd.)

The "Complete Conjecture" (Beelen - Datta - G, 2018)

For $1 \leq d < q$ and $1 \leq r \leq \binom{m+d}{d}$, if i, j are as above, then

$$e_r(d, m) = H_j(d-1, m-i) + p_{m-i-1}.$$

This reduces to the "Incomplete Conjecture" if $1 \leq r \leq \binom{m+d-1}{d-1}$.

More Recent Results (Contd.)

The "Complete Conjecture" (Beelen - Datta - G, 2018)

For $1 \le d < q$ and $1 \le r \le \binom{m+d}{d}$, if i, j are as above, then

$$e_r(d,m) = H_j(d-1, m-i) + p_{m-i-1}.$$

This reduces to the "Incomplete Conjecture" if $1 \le r \le \binom{m+d-1}{d-1}$.

The "Complete Conjecture" Version II (Beelen - Datta - G, 2018)

For $1 \le d < q$ and $1 \le r \le \binom{m+d}{d}$,

$$e_r(d,m) = p_{s_d - d} + \lfloor q^{s_{d-1}-d+1} \rfloor + \lfloor q^{s_{d-2}-d+2} \rfloor + \cdots + \lfloor q^{s_1 - 1} \rfloor,$$

where $s_1, \ldots, s_d$ are unique integers with $s_d > s_{d-1} > \cdots > s_1 \ge 0$ satisfying the *d*-binomial expansion:

$$\binom{m+d}{d} - r = \binom{s_d}{d} + \binom{s_{d-1}}{d-1} + \cdots + \binom{s_1}{1}.$$

More Recent Results (Contd.)

The conjectured value is, in fact, always a lower bound.

Theorem (Lower Bound)

For m, d, r, i, j as above,

$$e_r(d, m) \geq H_j(d-1, m-i) + p_{m-i-1}$$

There is an upper bound using a "projective variant" of $H_r(d, m)$.

Theorem (Upper Bound)

For m, d, r as above,

$$e_r(d, m) \leq K_r(d, m), \quad \text{where} \quad K_r(d, m) := \sum_{i=0}^{m} a_i p_{m-i-1},$$

and where $(a_0, a_1, \ldots, a_m)$ is the r-th element, in descending lexicographic order, of the set of all $(m+1)$-tuples $(b_0, b_1, \ldots, b_m)$ of nonnegative integers satisfying $b_0 + b_1 + \cdots + b_m = d$.

Current State of the New Conjecure

We know that the new conjecture is valid in many, but not all, cases. The major ones are summarized below.

Theorem (Partial Validity of the Complete Conjecture)

The "complete conjecture" holds in the affirmative for

$$1 \le r \le \binom{m+2}{2}$$

and for $(m+1)d$ additional values of r, namely, for

$$r = \binom{m+d-1}{d-1} + \cdots + \binom{m+d-i}{d-1} - t$$

where

$$1 \le i \le m+1 \quad \text{and} \quad 0 \le t \le d-1.$$

In fact, $e_r(d,m) = p_{m-i} + t$ for above $(m+1)d$ values of r.

On the proof of the new conjectures and results

Here we use a completely new approach that uses:

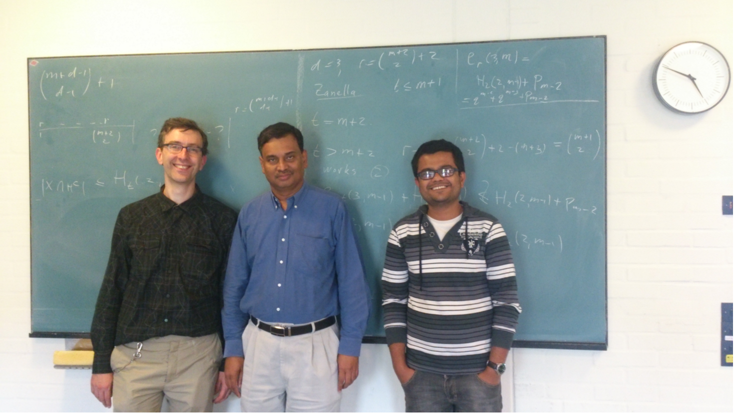
- Results from extremal combinatorics such as Clements-Lindström Theorem and its variants and extensions
- Notions of projective reduction of polynomials with coefficients in $\mathbb{F}_q$ and a projective footprint bound
- Hilbert functions and vanishing ideals of projective spaces over finite fields
- Macaulay expansions or d-binomial expansions of integers.

For more details, see the preparatory paper in *Acta Math. Sinica* (2019) and the preprint `arXiv:1807.01683` (2018), both joint with Peter Beelen and Mrinmoy Datta.

Remark.

The general problem of explicit determination of $e_r(d, m)$ remains open and can be a good challenge for young researchers!

Thank you for your attention!



For articles related to my (joint) work mentioned in this talk, see:
http://www.math.iitb.ac.in/∼srg/Papers.html
https://arxiv.org/a/ghorpade_s_1.html

Last e-mail to me from Alexey Zykin

Alexey Zykin <alzykin@gmail.com> Sat, Sep 17, 2016 at 7:50 AM
To: Sudhir Ghorpade <sudhirghorpade@gmail.com>

Dear Sudhir,
Thank you for your positive reply! Taking into account your availability, scheduling my visit to start in the beginning August would possibly be the best idea, since there is a summer school that I organize from July 24 to August 1 in Yaroslavl, Russia, and I am practically free after that. I am still in Tahiti, though I tend to come to Moscow for at least two months per year. Right now, I have several projects going on mostly in collaboration: one with Philippe Lebacque on M-functions related to modular forms, one with Alexey Zaytsev on counting points of high degree in recursive towers, one with Stphane Ballet on fast multiplication from Shimura curves, and yet another one with Fabien Pazuki on small heights of points on abelian varieties over function fields and number fields. Do codes form Grassmannian varieties constitute your principal subject of interest these days? Do you have any preferences for the potential topic of my lectures ? I am looking forward to coming to India and discussing mathematics with you!

Best regards, Alexey.

Effective Lang-Weil and Extended Deligne Inequality

Let X be an irreducible projective algebraic variety in $\mathbb{P}^m$ defined over $\mathbb{F}_q$ by r equations of degrees $d_1, \ldots, d_r$. Let $n = \dim X$, $\mathbf{d} = (d_1, \ldots, d_r)$, and $\delta = \max\{d_1, \ldots, d_m\}$. The results of G-Lachad (2002) alluded to earlier are the following.

- (Effective Lang-Weil Inequality) If $d = \deg X$, then
$$\Big| |X(\mathbb{F}_q)| - p_n \Big| \leq (d-1)(d-2)q^{n-(1/2)} + C\, q^{n-1},$$
where C is a constant independent of q, and in fact,
$$C \leq 9 \times 2^r \times (r\delta + 3)^{m+1}. \tag{3}$$
- (Extended Deligne Inequality) Assume that X is a complete intersection (so that we may take $r = m - n$). Suppose $s \in \mathbb{Z}$ with $\dim \mathrm{sing}\, X \leq s \leq n - 1$. Then
$$\Big| |X(\mathbb{F}_q)| - p_n \Big| \leq b'_{n-s-1}(m-s-1, \mathbf{d})\, q^{(n+s+1)/2} + C\, q^{(n+s)/2},$$
where C is a constant independent of q. Also $C = 0$ if X is nonsingular, and C satisfies (3) if $s \geq 0$.

Connection with Coding Theory

Here is a quick review of basics about (linear) codes.

- $[n,k]_q$-code: a k-dimensional subspace C of $\mathbb{F}_q^n$.
- Hamming weight of $c = (c_1, \ldots, c_n) \in \mathbb{F}_q^n$:

$$w_H(c) := \#\{i : c_i \neq 0\}.$$

- Hamming weight of a subcode D of C:

$$w_H(D) := \#\{i : \exists\ c = (c_1, \ldots, c_n) \in D \text{ with } c_i \neq 0\}.$$

- Minimum distance of a (linear) code C:

$$d(C) := \min\{w_H(c) : c \in C,\ c \neq 0\}.$$

- The r^{th} higher weight of C $(1 \le r \le k)$:

$$d_r(C) := \min\{w_H(D) : D \subseteq C,\ \dim D = r\}.$$

- C is nondegenerate if $C \not\subseteq$ coordinate hyperplane of $\mathbb{F}_q^n$, or equivalently, if $d_k(C) = n$.

A Nice Example: Reed-Muller Codes

Write $\mathbb{A}^m(\mathbb{F}_q) := \mathbb{F}_q^m = \{P_1, P_2, \dots, P_{q^m}\}$. Consider the evaluation map of the polynomial ring in m variables:

$$\begin{aligned} \mathrm{Ev} : \mathbb{F}_q[X_1, \dots, X_m] &\to \mathbb{F}_q^{q^m} \\ f &\longmapsto (f(P_1), \dots, f(P_{q^m})), \end{aligned}$$

The d^{th} order generalized Reed-Muller code of length q^m:

$$\mathrm{RM}(d, m) := \mathrm{Ev}\left(\mathbb{F}_q[X_1, \dots, X_m]_{\leq d}\right) \quad \text{for } d < q.$$

This has dimension $\binom{m+d}{d}$ and minimum distance $(q-d)q^{m-1}$.

More generally, one can consider $\mathrm{RM}(d, m)$ for $d \leq m(q-1)$, defined in a similar way, but in this case the formulas for the dimension and the minimum distance are a little more complicated:

$$\dim \mathrm{RM}(d, m) = \sum_{i=0}^{d} \sum_{j=0}^{m} (-1)^j \binom{m}{j} \binom{m+i-jq-1}{i-jq}$$

Minimum distance & Higher Weights of Reed-Muller Codes

The minimum distance of d^{th} order generalized Reed-Muller code of length q^m is given by

$$d\,(\mathrm{RM}(d,m)) = (R+1)q^Q,$$

where $Q, R \in \mathbb{Z}$ are such that $m(q-1) - d = Q(q-1) + R$ and $0 \le R < q-1$. The Heijnen-Pelikaan Theorem corresponds precisely to the determination of the r^{th} higher weight of (affine) Reed-Muller code $\mathrm{RM}(d,m)$. Indeed,

$$d_r\,(\mathrm{RM}(d,m)) = q^m - \max \#V(f_1,\ldots,f_r), \quad 1 \le r \le \binom{m+d}{d},$$

where the maximum is over all families of r linearly independent polynomials $f_1,\ldots,f_r$ in $\mathbb{F}_q[X_1,\ldots,X_m]$ of degree $\le d$.

Side Remark: An interesting new variant of R-M codes, called affine Grassmann codes, has recently been studied. cf. Beelen, Ghorpade, and Høholdt, *IEEE Trans. Inform. Theory*, **56** (2010), 3166–3176 and **58** (2012), 3843–3855.

Projective Reed-Muller Codes

Write $\mathbb{P}^m(\mathbb{F}_q) = \{P_1, P_2, \dots, P_{p_m}\}$, where the P_j are definite representatives in $\mathbb{F}_q^{m+1}$ of points in $\mathbb{P}^m(\mathbb{F}_q)$ chosen in such a way that the first nonzero coordinate is 1. Consider the evaluation map of the polynomial ring in $m+1$ variables:

$$\begin{aligned}\mathrm{Ev} : \mathbb{F}_q[X_0, X_1, \dots, X_m] &\to \mathbb{F}_q^{p_m} \\ F &\longmapsto \left(F(P_1), \dots, F(P_{p_m})\right),\end{aligned}$$

The$q$-ary d^{th} order projective Reed-Muller code of length p_m:

$$\mathrm{PRM}_q(d, m) := \mathrm{Ev}\left(\mathbb{F}_q[X_0, X_1, \dots, X_m]_d\right) \quad \text{for } d < q.$$

This has dimension $\binom{m+d}{d}$ and minimum distance

$$p_m - \left(dq^{m-1} + p_{m-2}\right) = q^{m-1}(q - d + 1).$$

For $d \le q$, determining the higher weights d_r of $\mathrm{PRM}_q(d, m)$ corresponds precisely to determining $e_r(d, m)$, since

$$d_r\left(\mathrm{PRM}_q(d, m)\right) = p_m - e_r(d, m) \quad \text{for } 1 \le d \le q.$$

The case $d > q$

Like the Reed-Muller Codes, the Projective Reed Muller codes $\mathrm{PRM}_q(d, m)$ are defined more generally when $1 \leq d \leq m(q-1)$, and $k_d := \dim_{\mathbb{F}_q} \mathrm{PRM}_q(d, m)$ is given, in general, by the Mercier-Rolland formula:

$$k_d = \binom{m+d}{d} - \sum_{j=2}^{m+1} (-1)^j \binom{m+1}{j} \sum_{i=1}^{j-1} \binom{m+d-i+(i-j)q}{d-i+(i-j)q},$$

or equivalently, by the Sørensen formula:

$$k_d = \sum_{\substack{t=1 \\ t \equiv d \pmod{q-1}}}^{d} \left(\sum_{j=0}^{m+1} (-1)^j \binom{m+1}{j} \binom{t-jq+m}{t-jq} \right).$$

If $d \leq q$, then k_d reduces to $\binom{m+d}{d}$, but in general it can be smaller. Further,

$$d_r(\mathrm{PRM}_q(d, m)) = e_{r+r_d}(d, m) \quad \text{for } r = 1, \ldots, k_d,$$

where $r_d = \binom{m+d}{d} - k_d$. For more on this, see: `arXiv:1807.01683v2 [math.AG]` (July 2018).

Thank you!