Estimates on the average cardinality of the value set of general families of univariate polynomials over a finite field.

Melina Privitelli

Universidad Nacional de General Sarmiento
Buenos Aires, Argentina

Work in collaboration with Guillermo Matera and Mariana Pérez

XXI Coloquio Latinoamericano de Álgebra
Universidad de Buenos Aires
July 2016

Notations

$\mathbb{F}_q$ finite field of q elements,

$\overline{\mathbb{F}}_q$ algebraic closure of $\mathbb{F}_q$,

$\mathcal{P}_d$ the set of monic polynomials of $\mathbb{F}_q[T]$ of degree d.

Given $f \in \mathbb{F}_q[T]$, its value set is defined as $\{f(c) : c \in \mathbb{F}_q\}$. We denote its cardinality by $\mathcal{V}(f)$.

Notations

$\mathbb{F}_q$ finite field of q elements,

$\overline{\mathbb{F}}_q$ algebraic closure of $\mathbb{F}_q$,

$\mathcal{P}_d$ the set of monic polynomials of $\mathbb{F}_q[T]$ of degree d.

Given $f \in \mathbb{F}_q[T]$, its value set is defined as $\{f(c) : c \in \mathbb{F}_q\}$. We denote its cardinality by $\mathcal{V}(f)$.

Birch and Swinnerton–Dyer [Acta Arith, 1959]: for a "generic" $f \in \mathcal{P}_d$,

$$\mathcal{V}(f) = \mu_d q + O(q^{1/2}),$$

$\mu_d := \sum_{j=1}^{d} \frac{(-1)^{j-1}}{j!} \approx 0,6321...$

S. Uchiyama and S. D. Cohen study the average cardinality of value sets.

S. Uchiyama and S. D. Cohen study the average cardinality of value sets.

Cohen [Glasgow MJ, 1973] proves that

$$\frac{1}{|\mathcal{P}_d|} \sum_{f \in \mathcal{P}_d} \mathcal{V}(f) = \mu_d q + \mathcal{O}(1).$$

S. Uchiyama and S. D. Cohen study the average cardinality of value sets.

Cohen [Glasgow MJ, 1973] proves that

$$\frac{1}{|\mathcal{P}_d|}\sum_{f\in\mathcal{P}_d}\mathcal{V}(f)=\mu_d q+\mathcal{O}(1).$$

Question: What can we say on average for families $\mathcal{A}\subset\mathcal{P}_d$?

S. Uchiyama and S. D. Cohen study the average cardinality of value sets.

Cohen [Glasgow MJ, 1973] proves that

$$\frac{1}{|\mathcal{P}_d|}\sum_{f\in\mathcal{P}_d}\mathcal{V}(f)=\mu_d q+\mathcal{O}(1).$$

Question: What can we say on average for families $\mathcal{A}\subset\mathcal{P}_d$?
Example: Polynomials with s prescribed coefficients

$$\mathcal{A}_s=\{f=T^d+a_{d-1}T^{d-1}+\cdots+a_0:\ a_{d-s-1},\ldots,a_0\in\mathbb{F}_q\}.$$

S. Uchiyama and S. D. Cohen study the average cardinality of value sets.

Cohen [Glasgow MJ, 1973] proves that

$$\frac{1}{|\mathcal{P}_d|}\sum_{f\in\mathcal{P}_d}\mathcal{V}(f)=\mu_d q+\mathcal{O}(1).$$

Question: What can we say on average for families $\mathcal{A}\subset\mathcal{P}_d$?
Example: Polynomials with s prescribed coefficients

$$\mathcal{A}_s=\{f=T^d+a_{d-1}T^{d-1}+\cdots+a_0:\ a_{d-s-1},\ldots,a_0\in\mathbb{F}_q\}.$$

Cohen [J London MS, 1972]: for $\mathrm{char}(\mathbb{F}_q)>d$

$$\mathcal{V}(\mathcal{A}_s)=\frac{1}{|\mathcal{A}_s|}\sum_{f\in\mathcal{A}_s}\mathcal{V}(f)=\mu_d q+\mathcal{O}(q^{1/2}).$$

In a joint work with E. Cesaratto, G. Matera, and M. Pérez [JCTA,2014]:

Theorem: if $s \leq d/2$ and any $\mathrm{char}(\mathbb{F}_q)$

$$|\mathcal{V}(\mathcal{A}_s) - \mu_d q| \leq c_1(d),$$

where $c_1(d)$ is explicit and has a "good behavior".

In a joint work with E. Cesaratto, G. Matera, and M. Pérez [JCTA,2014]:

Theorem: if $s \leq d/2$ and any $\mathrm{char}(\mathbb{F}_q)$

$$|\mathcal{V}(\mathcal{A}_s) - \mu_d q| \leq c_1(d),$$

where $c_1(d)$ is explicit and has a "good behavior".

In a joint work with G. Matera, and M. Pérez [Acta Arith.,2014]:

Theorem: if $s \leq d-3$ and $\mathrm{char}(\mathbb{F}_q) > 2$

$$|\mathcal{V}(\mathcal{A}_s) - \mu_d q| \leq c_2(d) q^{1/2},$$

where $c_2(d)$ is explicit.

Motivation:

$V(\mathcal{A}_s)$ is related to the analysis of the cost of algorithms for computing $\mathbb{F}_q$–rational zeros of polynomials in $\mathbb{F}_q[X_1, \ldots, X_n]$ based on search on vertical strips (SVS).

The asymptotic behavior of the SVS algorithm is determined by that of $V(\mathcal{A}_s)$.

Motivation:

$V(\mathcal{A}_s)$ is related to the analysis of the cost of algorithms for computing $\mathbb{F}_q$–rational zeros of polynomials in $\mathbb{F}_q[X_1, \ldots, X_n]$ based on search on vertical strips (SVS).

The asymptotic behavior of the SVS algorithm is determined by that of $V(\mathcal{A}_s)$.

Cohen [J London MS, 1972] it is shown that, for a linear family $\mathcal{A} \subset \mathcal{P}_d$ with certain conditions and $char(\mathbb{F}_q) > d$,

$$\mathcal{V}(\mathcal{A}) = \frac{1}{|\mathcal{A}|} \sum_{f \in \mathcal{A}} \mathcal{V}(f) = \mu_d q + \mathcal{O}(q^{1/2}).$$

Let d, m be positive integers with $m+2 \leq d \leq q$, and let $G_1, \ldots, G_m \in \mathbb{F}_q[A_{d-1}, \ldots, A_0]$ be polynomials of degree $d_1, \ldots, d_m$.

Let d, m be positive integers with $m+2 \leq d \leq q$, and let $G_1, \ldots, G_m \in \mathbb{F}_q[A_{d-1}, \ldots, A_0]$ be polynomials of degree $d_1, \ldots, d_m$.

Let $\mathcal{A} := \mathcal{A}(G_1, \ldots, G_m) \subset \mathcal{P}_d$ be the family defined as:

$$\mathcal{A} := \left\{ T^d + \sum_{j=1}^{d-1} a_j T^j : \ G_i(a_{d-1}, \ldots, a_1) = 0 \ (1 \leq i \leq m) \right\}.$$

Let d, m be positive integers with $m+2 \leq d \leq q$, and let $G_1, \ldots, G_m \in \mathbb{F}_q[A_{d-1}, \ldots, A_0]$ be polynomials of degree $d_1, \ldots, d_m$.

Let $\mathcal{A} := \mathcal{A}(G_1, \ldots, G_m) \subset \mathcal{P}_d$ be the family defined as:

$$\mathcal{A} := \left\{ T^d + \sum_{j=1}^{d-1} a_j T^j : \ G_i(a_{d-1}, \ldots, a_1) = 0 \ (1 \leq i \leq m) \right\}.$$

Our Aim: establish rather general conditions on $G_1, \ldots, G_m$ under which $\mathcal{V}(\mathcal{A}) = \mu_d q + \mathcal{O}(q^{1/2})$.

- Not to impose restrictions on $\mathrm{char}(\mathbb{F}_q)$,
- Obtain explicit estimates.

Our Approach: Apply methods of algebraic geometry, after a simple combinatorial reduction.

Our Approach: Apply methods of algebraic geometry, after a simple combinatorial reduction.

For $f \in \mathcal{A}$,

$$\mathcal{V}(f) = \left|\{b \in \mathbb{F}_q : \ (f+b) \text{ has at least one root in } \mathbb{F}_q\}\right|.$$

Our Approach: Apply methods of algebraic geometry, after a simple combinatorial reduction.

For $f \in \mathcal{A}$,

$$\mathcal{V}(f) = \Big|\{b \in \mathbb{F}_q : \ (f+b) \text{ has at least one root in } \mathbb{F}_q\}\Big|.$$

Let $\mathcal{N}(f) = \Big|\{\text{zeros of } f \text{ in } \mathbb{F}_q\}\Big|$. Then

$$\sum_{f \in \mathcal{A}} \mathcal{V}(f) = \Big|\{f + b \in \mathcal{A} + \mathbb{F}_q : \ \mathcal{N}(f+b) > 0\}\Big|.$$

Our Approach: Apply methods of algebraic geometry, after a simple combinatorial reduction.

For $f \in \mathcal{A}$,

$$\mathcal{V}(f) = \Big|\{b \in \mathbb{F}_q : \ (f+b) \text{ has at least one root in } \mathbb{F}_q\}\Big|.$$

Let $\mathcal{N}(f) = \Big|\{\text{zeros of } f \text{ in } \mathbb{F}_q\}\Big|$. Then

$$\sum_{f \in \mathcal{A}} \mathcal{V}(f) = \Big|\{f+b \in \mathcal{A}+\mathbb{F}_q : \ \mathcal{N}(f+b) > 0\}\Big|.$$

Furthermore,

$$\Big|\{f+b \in \mathcal{A}+\mathbb{F}_q : \ \mathcal{N}(f+b) > 0\}\Big| = \Big|\bigcup_{x \in \mathbb{F}_q} \mathcal{S}_{\{x\}}^{\mathcal{A}+\mathbb{F}_q}\Big|,$$

where $\mathcal{S}_{\{x\}}^{\mathcal{A}+\mathbb{F}_q} = \{f+b \in \mathcal{A}+\mathbb{F}_q : \ f(x) = 0\}$.

Therefore, by the inclusion–exclusion principle we have that

$$\mathcal{V}(\mathcal{A}) = \frac{1}{|\mathcal{A}|}\left|\bigcup_{x\in\mathbb{F}_q} \mathcal{S}^{\mathcal{A}+\mathbb{F}_q}_{\{x\}}\right| = \frac{1}{|\mathcal{A}|}\sum_{r=1}^{q}(-1)^{r-1}\sum_{\mathcal{X}_r\subset\mathbb{F}_q}|\mathcal{S}^{\mathcal{A}+\mathbb{F}_q}_{\mathcal{X}_r}|,$$

where $\mathcal{X}_r := \{x_1, \ldots, x_r\} \subset \mathbb{F}_q$.

Therefore, by the inclusion–exclusion principle we have that

$$\mathcal{V}(\mathcal{A}) = \frac{1}{|\mathcal{A}|}\left|\bigcup_{x\in\mathbb{F}_q} \mathcal{S}_{\{x\}}^{\mathcal{A}+\mathbb{F}_q}\right| = \frac{1}{|\mathcal{A}|}\sum_{r=1}^{q}(-1)^{r-1}\sum_{\mathcal{X}_r\subset\mathbb{F}_q}|\mathcal{S}_{\mathcal{X}_r}^{\mathcal{A}+\mathbb{F}_q}|,$$

where $\mathcal{X}_r := \{x_1, \ldots, x_r\} \subset \mathbb{F}_q$.

For $r > d$, $\left|\mathcal{S}_{\mathcal{X}_r}^{\mathcal{A}+\mathbb{F}_q}\right| = 0$.

Therefore, by the inclusion–exclusion principle we have that

$$\mathcal{V}(\mathcal{A}) = \frac{1}{|\mathcal{A}|}\left|\bigcup_{x\in\mathbb{F}_q} \mathcal{S}_{\{x\}}^{\mathcal{A}+\mathbb{F}_q}\right| = \frac{1}{|\mathcal{A}|}\sum_{r=1}^{q}(-1)^{r-1}\sum_{\mathcal{X}_r\subset\mathbb{F}_q}|\mathcal{S}_{\mathcal{X}_r}^{\mathcal{A}+\mathbb{F}_q}|,$$

where $\mathcal{X}_r := \{x_1,\ldots,x_r\} \subset \mathbb{F}_q$.

For $r > d$, $\left|\mathcal{S}_{\mathcal{X}_r}^{\mathcal{A}+\mathbb{F}_q}\right| = 0$.

Problem: determine the asymptotic behavior of

$$\mathcal{S}_r := \sum_{\mathcal{X}_r\subset\mathbb{F}_q}|\mathcal{S}_{\mathcal{X}_r}^{\mathcal{A}+\mathbb{F}_q}|,$$

for each $1 \le r \le d$.

The number:

$$\mathcal{S}_r = \sum_{\mathcal{X}_r \subset \mathbb{F}_q} |\mathcal{S}_{\mathcal{X}_r}^{\mathcal{A}+\mathbb{F}_q}| = |\{(\mathcal{X}_r, f) : \ \mathcal{X}_r \subset \mathbb{F}_q, f \in \mathcal{A} + \mathbb{F}_q, \ f|_{\mathcal{X}_r} = 0\}|.$$

We consider the incidence variety

$$V_r := \{(\mathcal{X}_r, f) : \ \mathcal{X}_r \subset \mathbb{F}_q, f \in \mathcal{A} + \mathbb{F}_q, \ f|_{\mathcal{X}_r} = 0\}.$$

Determine the asymptotic behavior of the number of $\mathbb{F}_q$-rational points of the incidence variety V_r.

The number:

$$\mathcal{S}_r = \sum_{\mathcal{X}_r \subset \mathbb{F}_q} |\mathcal{S}_{\mathcal{X}_r}^{\mathcal{A}+\mathbb{F}_q}| = |\{(\mathcal{X}_r, f) : \ \mathcal{X}_r \subset \mathbb{F}_q, f \in \mathcal{A} + \mathbb{F}_q, \ f|_{\mathcal{X}_r} = 0\}|.$$

We consider the incidence variety

$$V_r := \{(\mathcal{X}_r, f) : \ \mathcal{X}_r \subset \mathbb{F}_q, f \in \mathcal{A} + \mathbb{F}_q, \ f|_{\mathcal{X}_r} = 0\}.$$

Determine the asymptotic behavior of the number of $\mathbb{F}_q$-rational points of the incidence variety V_r.

We obtain $r + m$ equations defining V_r.

Γ_r = the set of solutions of these equations in $\overline{\mathbb{F}}_q$.

The number:

$$\mathcal{S}_r = \sum_{\mathcal{X}_r \subset \mathbb{F}_q} |\mathcal{S}_{\mathcal{X}_r}^{\mathcal{A}+\mathbb{F}_q}| = |\{(\mathcal{X}_r, f) : \ \mathcal{X}_r \subset \mathbb{F}_q, f \in \mathcal{A} + \mathbb{F}_q, \ f|_{\mathcal{X}_r} = 0\}|.$$

We consider the incidence variety

$$V_r := \{(\mathcal{X}_r, f) : \ \mathcal{X}_r \subset \mathbb{F}_q, f \in \mathcal{A} + \mathbb{F}_q, \ f|_{\mathcal{X}_r} = 0\}.$$

Determine the asymptotic behavior of the number of $\mathbb{F}_q$-rational points of the incidence variety V_r.

We obtain $r + m$ equations defining V_r.

Γ_r = the set of solutions of these equations in $\overline{\mathbb{F}}_q$.

We study the singular points of Γ_r.

Let $\mathcal{C}$ be the set of $f = T^d + a_{d-1}T^{d-1} + \cdots + a_0 \in \overline{\mathbb{F}}_q[T]$ with

$$G_1(a_{d-1}, \ldots, a_0) = 0, \cdots, G_m(a_{d-1}, \ldots, a_0) = 0.$$

Let $\mathcal{C}$ be the set of $f = T^d + a_{d-1}T^{d-1} + \cdots + a_0 \in \overline{\mathbb{F}}_q[T]$ with

$$G_1(a_{d-1}, \ldots, a_0) = 0, \cdots, G_m(a_{d-1}, \ldots, a_0) = 0.$$

A singular point of Γ_r arises from:

- a singular point of V, where $V := V(G_1, \ldots, G_m)$, or
- a polynomial $f \in \mathcal{C}$ which is non square–free.

Let $\mathcal{C}$ be the set of $f = T^d + a_{d-1}T^{d-1} + \cdots + a_0 \in \overline{\mathbb{F}}_q[T]$ with

$$G_1(a_{d-1}, \ldots, a_0) = 0, \cdots, G_m(a_{d-1}, \ldots, a_0) = 0.$$

A singular point of Γ_r arises from:

- a singular point of V, where $V := V(G_1, \ldots, G_m)$, or
- a polynomial $f \in \mathcal{C}$ which is non square–free.

This suggests:

- Establishing conditions on $G_1, \ldots, G_m$ in order to "control" the dimension of the singular locus of V,
- Studying the discriminant locus $\mathcal{D}(\mathcal{C})$ of $\mathcal{C}$.

Let $\mathcal{C}$ be the set of $f = T^d + a_{d-1}T^{d-1} + \cdots + a_0 \in \overline{\mathbb{F}}_q[T]$ with

$$G_1(a_{d-1}, \ldots, a_0) = 0, \cdots, G_m(a_{d-1}, \ldots, a_0) = 0.$$

A singular point of Γ_r arises from:

- a singular point of V, where $V := V(G_1, \ldots, G_m)$, or
- a polynomial $f \in \mathcal{C}$ which is non square–free.

This suggests:

- Establishing conditions on $G_1, \ldots, G_m$ in order to "control" the dimension of the singular locus of V,
- Studying the discriminant locus $\mathcal{D}(\mathcal{C})$ of $\mathcal{C}$.

We shall need further to consider $\mathcal{S}_1(\mathcal{C})$, the first subdiscriminant locus of $\mathcal{C}$,

$$S_1(\mathcal{C}) = \{f \in \mathcal{C} : \ \mathrm{Subdisc}(f) = 0\}, \quad \mathrm{Subdisc}(f) := \mathrm{Subres}(f, f').$$

Recall $V = V(G_1, \ldots, G_m) \subset \mathbb{A}^d$.

Recall $V = V(G_1, \ldots, G_m) \subset \mathbb{A}^d$.

- (H_1) $G_1, \ldots, G_m$ form a regular sequence and generate a radical ideal of $\mathbb{F}_q[A_{d-1}, \ldots, A_0]$.
- (H_2) The variety $V \subset \mathbb{A}^d$ is normal.
- (H_3) Let $G_1^{d_1}, \ldots, G_m^{d_m}$ denote the homogeneous parts of higher degree of $G_1, \ldots, G_m$ satisfy (H_1) and (H_2).
- (H_4) $\mathcal{D}(\mathcal{C})$ has codimension 1 in V and $\mathcal{D}(\mathcal{C}) \cap \mathcal{S}_1(\mathcal{C})$ has codimension 2 in V.

We obtain the following result:

Theorem: Γ_r is a complete intersection and the singular locus of Γ_r has codimension at least 2.

We obtain the following result:

Theorem: Γ_r is a complete intersection and the singular locus of Γ_r has codimension at least 2.

We use the following result (joint work with A. Cafure and G. Matera [FFA, 2015]):

Theorem: Let $F_1, \ldots, F_{n-r} \in \mathbb{F}_q[X_0, \ldots, Xn]$ be homogeneous polynomials of degrees $d_1, \ldots, d_{n-r}$ which define a normal complete intersection $V \subset \mathbb{P}^n$ of degree δ. Let $D := \sum_{i=1}^{n-r}(d_i - 1)$ and $p_r := |\mathbb{P}^n(\mathbb{F}_q)|$. Then

$$\left||V(\mathbb{F}_q)| - p_r\right| \leq \delta(D-2) + 2q^{r-1/2} + 14D^2\delta^2 q^{r-1}.$$

We obtain the following result:

Theorem: Γ_r is a complete intersection and the singular locus of Γ_r has codimension at least 2.

We use the following result (joint work with A. Cafure and G. Matera [FFA, 2015]):

Theorem: Let $F_1, \ldots, F_{n-r} \in \mathbb{F}_q[X_0, \ldots, Xn]$ be homogeneous polynomials of degrees $d_1, \ldots, d_{n-r}$ which define a normal complete intersection $V \subset \mathbb{P}^n$ of degree δ. Let $D := \sum_{i=1}^{n-r}(d_i - 1)$ and $p_r := |\mathbb{P}^n(\mathbb{F}_q)|$. Then

$$\left||V(\mathbb{F}_q)| - p_r\right| \leq \delta(D-2) + 2q^{r-1/2} + 14D^2\delta^2 q^{r-1}.$$

This allows us to estimate the number of $\mathbb{F}_q$-rational points of Γ_r and then the asymptotic behavior of $\mathcal{S}_r$.

Theorem: Let $q > d \geq m + 2$. For any r with and $1 \leq r \leq d$, we have

$$\left|\mathcal{S}_r - \frac{q^{d-m}}{r!}\right| \leq \left(\delta_r D_r q^{\frac{1}{2}} + 15 D_r^2 \delta_r^2 + 4 r \delta_V\right) \frac{q^{d-m-1}}{r!},$$

where $\delta_r := \delta_V \frac{d!}{(d-r)!}$ and $D_r := D_v + rd - \frac{r(r+1)}{2}$.

Theorem: Let $q > d \geq m+2$. For any r with and $1 \leq r \leq d$, we have

$$\left|\mathcal{S}_r - \frac{q^{d-m}}{r!}\right| \leq \left(\delta_r D_r q^{\frac{1}{2}} + 15 D_r^2 \delta_r^2 + 4 r \delta_V\right) \frac{q^{d-m-1}}{r!},$$

where $\delta_r := \delta_V \frac{d!}{(d-r)!}$ and $D_r := D_v + rd - \frac{r(r+1)}{2}$.

- H_1, H_2 and $H_3 \Rightarrow |\mathcal{A}| = q^{d-m-1} + \mathcal{O}(q^{d-m-3/2})$.

Theorem: Let $q > d \geq m+2$. For any r with and $1 \leq r \leq d$, we have

$$\left|\mathcal{S}_r - \frac{q^{d-m}}{r!}\right| \leq \left(\delta_r D_r q^{\frac{1}{2}} + 15 D_r^2 \delta_r^2 + 4 r \delta_V\right) \frac{q^{d-m-1}}{r!},$$

where $\delta_r := \delta_V \frac{d!}{(d-r)!}$ and $D_r := D_v + rd - \frac{r(r+1)}{2}$.

- H_1, H_2 and $H_3 \Rightarrow |\mathcal{A}| = q^{d-m-1} + \mathcal{O}(q^{d-m-3/2})$.
- If $q > 16 D_V^2 \delta_V^2 (1 + 14 D_V \delta_V q^{-1/2})^2$ then $\frac{1}{2} q^{d-m-1} < |\mathcal{A}|$.

Theorem: Let $q > \max\left\{d, 16D_V^2\delta_V^2(1+14D_V\delta_V q^{-1/2})^2\right\}$ and $d \geq m+2$, then:

$$|\mathcal{V}(\mathcal{A}) - \mu_d\, q| \leq 2^d\delta_V(3D_V+d^2)q^{\frac{1}{2}} + 67\delta_V^2(D_V+2)^2\, d^{d+5}e^{2\sqrt{d}-d}.$$

Theorem: Let $q > \max\left\{d, 16D_V^2\delta_V^2(1+14D_V\delta_V q^{-1/2})^2\right\}$ and $d \geq m+2$, then:

$$|\mathcal{V}(\mathcal{A}) - \mu_d\, q| \leq 2^d\delta_V(3D_V+d^2)q^{\frac{1}{2}} + 67\delta_V^2(D_V+2)^2\, d^{d+5}e^{2\sqrt{d}-d}.$$

The asymptotic behavior of $\mathcal{V}(\mathcal{A})$

$$\mathcal{V}(\mathcal{A}) = \mu_d q + \mathcal{O}(q^{1/2}).$$

Two examples of families

Linear Families: $L_1, \ldots, L_m \in \mathbb{F}_q[A_{d-1}, \ldots, A_3]$ are polynomials of degree 1.

Assume that $L_1, \ldots, L_m$ are linearly independent.

$$\mathcal{A}_{\mathcal{L}} := \Big\{ T^d + \sum_{j=1}^{d-1} a_j T^j \in \mathbb{F}_q[T] : L_i(a_{d-1}, \ldots, a_3) = 0 \, (1 \leq i \leq m) \Big\}.$$

Two examples of families

Linear Families: $L_1, \ldots, L_m \in \mathbb{F}_q[A_{d-1}, \ldots, A_3]$ are polynomials of degree 1.

Assume that $L_1, \ldots, L_m$ are linearly independent.

$$\mathcal{A}_{\mathcal{L}} := \Big\{ T^d + \sum_{j=1}^{d-1} a_j T^j \in \mathbb{F}_q[T] : L_i(a_{d-1}, \ldots, a_3) = 0 \, (1 \leq i \leq m) \Big\}.$$

- It is clear that (H_1), (H_2) and (H_3) hold.
- (H_4) holds if $\mathrm{char}(\mathbb{F}_q) > 2$. It is a consequence of the absolutely irreducibility of the discriminant locus of $\mathcal{A}_{\mathcal{L}}$.

Theorem: If $\mathrm{char}(\mathbb{F}_q) > 2$ and $q > d \geq m + 2$, then

$$|\mathcal{V}(\mathcal{A}_{\mathcal{L}}) - \mu_d\, q| \leq 2^d d^2 q^{\frac{1}{2}} + 268 d^{d+5} e^{2\sqrt{d}-d}.$$

Theorem: If $\mathrm{char}(\mathbb{F}_q) > 2$ and $q > d \geq m + 2$, then

$$|\mathcal{V}(\mathcal{A}_{\mathcal{L}}) - \mu_d\, q| \leq 2^d d^2 q^{\frac{1}{2}} + 268 d^{d+5} e^{2\sqrt{d}-d}.$$

- We obtain simpler hypotheses on linear families which imply that the average value set has the expected behavior.
- We only require that $\mathrm{char}(\mathbb{F}_q) > 2$.
- Our estimate is explicit.

A nonlinear family of polynomials:

$\Pi_1, \ldots, \Pi_s$ are the first s elementary symmetric polynomials of $\mathbb{F}_q[A_{d-1}, \ldots, A_2]$.

$G_1, \ldots, G_m \in \mathbb{F}_q[A_{d-1}, \ldots, A_2]$ of the form $G_i := S_i(\Pi_1, \ldots, \Pi_s)$.

The weight function $\mathrm{wt} : \mathbb{F}_q[Y_1, \ldots, Y_s] \to \mathbb{N} : \mathrm{wt}(Y_i) := i$.

S_i^{wt} is the component of highest weight of S_i $(1 \leq i \leq s)$.

A nonlinear family of polynomials:

$\Pi_1, \ldots, \Pi_s$ are the first s elementary symmetric polynomials of $\mathbb{F}_q[A_{d-1}, \ldots, A_2]$.

$G_1, \ldots, G_m \in \mathbb{F}_q[A_{d-1}, \ldots, A_2]$ of the form $G_i := S_i(\Pi_1, \ldots, \Pi_s)$.

The weight function $\mathrm{wt} : \mathbb{F}_q[Y_1, \ldots, Y_s] \to \mathbb{N} : \mathrm{wt}(Y_i) := i$.

S_i^{wt} is the component of highest weight of S_i $(1 \leq i \leq s)$.

- $S_1, \ldots, S_m$ and $S_1^{\mathrm{wt}}, \ldots, S_m^{\mathrm{wt}}$ form regular sequences of $\mathbb{F}_q[Y_1, \ldots, Y_s]$,
- The Jacobian matrices of $S_1, \ldots, S_m$ and $S_1^{\mathrm{wt}}, \ldots, S_m^{\mathrm{wt}}$ with respect to $Y_1, \ldots, Y_s$ have full rank in $\mathbb{A}^s$.

$$\mathcal{A}_{\mathcal{N}} := \Big\{ T^d + \sum_{j=0}^{d-1} a_j T^j \in \mathbb{F}_q[T] : G_i(a_{d-1}, \ldots, a_2) = 0 \, (1 \leq i \leq m) \Big\}.$$

$$\mathcal{A}_{\mathcal{N}} := \Big\{ T^d + \sum_{j=0}^{d-1} a_j T^j \in \mathbb{F}_q[T] : G_i(a_{d-1}, \ldots, a_2) = 0 \, (1 \leq i \leq m) \Big\}.$$

- It is easy to verify that (H_1), (H_2) and (H_3) hold.
- (H_4) holds if $\mathrm{char}(\mathbb{F}_q)$ not dividing $d(d-1)$.

Varieties defined by polynomials of this type arise in several combinatorial problems over finite fields, for example:

- Coding theory: the study of deep holes of the standard Reed-Solomon code,
- Cryptography: the characterization of monomials defining an almost perfect nonlinear polynomial or differentially uniform mapping.

Thanks for your attention!