On divisors of sums of polynomials

László Mérai

Austrian Academy of Sciences
Johann Radon Institute for Computational and Applied Mathematics
Linz, Austria

August 30, 2022

Sums of polynomials

Let $\mathbb{F}_q$ be the finite field of size $|\mathbb{F}_q| = q$ of odd characteristic.

Let $\mathcal{A}, \mathcal{B} \subset \mathcal{M}_n \subset \mathbb{F}_q[T]$ be arbitrary subsets of monic polynomials.

We expect that the arithmetic properties of sumsets

$$\mathcal{A} + \mathcal{B} = \{A + B : A \in \mathcal{A}, B \in \mathcal{B}\},$$

have similar properties to those of $\mathcal{M}_n$.

In particular, what can we say about the arithmetic properties of $\mathcal{A} + \mathcal{B}$ by only knowing the sizes $|\mathcal{A}|, |\mathcal{B}|$?

Sum of polynomials

Let $\mathcal{A}, \mathcal{B} \subset \mathcal{M}_n$ be arbitrary subsets.

For a polynomial $F \in \mathbb{F}_q[X]$, let

$$\mathrm{D}(F) = \max\{\deg P : P \mid F,\ P \text{ is irreducible}\}.$$

We expect, that

$$\mathrm{D}(A + B) : A \in \mathcal{A}, B \in \mathcal{B}$$

cannot be all small.

For integers, see works of Balog, Ruzsa, Sárközy, Stewart, ...

The result

Let

$$\mathrm{D}(F) = \max\{\deg P : P \mid F,\ P \text{ is irreducible}\}.$$

and for $\mathcal{A}, \mathcal{B} \subset \mathcal{M}_n$

$$\sigma = \sigma(\mathcal{A}, \mathcal{B}) = \frac{(|\mathcal{A}||\mathcal{B}|)^{1/2}}{q^n}, \quad 0 \le \sigma \le 1.$$

Theorem

Let $\mathcal{A}, \mathcal{B} \subset \mathcal{M}_n$ and assume, that $(|\mathcal{A}||\mathcal{B}|)^{1/2} \ge q^{(6/7+\varepsilon)n}$. Then, there exist $\gg |\mathcal{A}||\mathcal{B}|/n$ polynomials $A \in \mathcal{A}$, $B \in \mathcal{B}$ such that

$$\mathrm{D}(A+B) \ge n - \log_q \sigma^{-1} - \log_q \log_q \log_q \sigma^{-1} - \frac{c}{\log q} - 1.$$

Trivial upper bound: $\mathrm{D}(A+B) \le n$.

The result

Let

$$\mathrm{D}(F) = \max\{\deg P : P \mid F,\ P \text{ is irreducible}\}.$$

and for $\mathcal{A}, \mathcal{B} \subset \mathcal{M}_n$

$$\sigma = \sigma(\mathcal{A}, \mathcal{B}) = \frac{(|\mathcal{A}||\mathcal{B}|)^{1/2}}{q^n}, \quad 0 \le \sigma \le 1.$$

Corollary

Let $\mathcal{A}, \mathcal{B} \subset \mathcal{M}_n$ and assume, that $|\mathcal{A}|, |\mathcal{B}| \gg q^n$, then there are polynomials $A \in \mathcal{A}$, $B \in \mathcal{B}$, such that

$$\mathrm{D}(A + B) \ge n - c.$$

The result is sharp apart from constants:
Let $\mathcal{A}, \mathcal{B} \subset \mathbb{F}_q[T]$ are sets s.t. $T \mid A, B$ for all $A \in \mathcal{A}, B \in \mathcal{B}$. Then $\mathrm{D}(A + B) \le n - 1$.

The method

The proof uses the Hardy–Littlewood circle method.

For $F \in \mathbb{F}_q[T]$, define $|F| = q^{\deg F}$ (with the convention $|0| = 0$).
Let

$$\mathbb{F}_q((T^{-1})) = \mathbb{K}_\infty = \left\{ \xi = \sum_{i \le k} x_i T^i, x_i \in \mathbb{F}_q, k \in \mathbb{Z} \right\}.$$

We extend $|\cdot|$ to $\mathbb{K}_\infty$ in a natural way. Then $\mathbb{K}_\infty$ is complete with respect to $|\cdot|$.
Define the unit interval

$$\mathbf{T} = \{\xi : |\xi| < 1\} = \left\{ \sum_{i=-\infty}^{-1} x_i T^i, x_i \in \mathbb{F}_q \right\}.$$

We define the measure μ on $\mathbf{T}$ by

$$\mu\left(\xi : x_{-1} = r_{-1}, \ldots, x_{-k} = r_{-k}\right) = \frac{1}{q^k}.$$

Then $\mu(\mathbf{T}) = 1$.

The method

For $\xi \in \mathbb{K}_\infty$ (i.e. $\xi = \sum_{i \le k} x_i T^i$) let

$$\mathbf{e}(\xi) = \exp\left(\frac{2\pi i}{p}\mathrm{tr}_{\mathbb{F}_q}(x_{-1})\right),$$

where $p = \mathrm{char}(\mathbb{F}_q)$ and $\mathrm{tr}_{\mathbb{F}_q} : \mathbb{F}_q \to \mathbb{F}_p$ is the trace.

Then $\mathbf{e} : \mathbb{K}_\infty \to \mathbb{C}^*$ is an additive character.

We have the orthogonality

$$\int_{\mathbf{T}} \mathbf{e}(\xi A) \mathrm{d}\mu(\xi) = \begin{cases} 1 & \text{if } A = 0, \\ 0 & \text{if } A \neq 0 \end{cases}$$

for $A \in \mathbb{F}_q[T]$.

The method

Write

$$f_{\mathcal{A}}(\xi) = \sum_{A \in \mathcal{A}} \mathbf{e}(A\xi) \quad f_{\mathcal{B}}(\xi) = \sum_{B \in \mathcal{B}} \mathbf{e}(B\xi).$$

Then

$$f_{\mathcal{A}}(\xi) f_{\mathcal{B}}(\xi) = \sum_{A \in \mathcal{A}, B \in \mathcal{B}} \mathbf{e}((A+B)\xi) = \sum_{G \in \mathcal{M}_n} u_G \mathbf{e}(G\xi),$$

where $u_G > 0$ iff $G \in \mathcal{A} + \mathcal{B}$.

Let j be a positive integer, put

$$\mathcal{S} = \{S \in \mathcal{M}_n : \mathrm{D}(S) = n - j\}.$$

and define

$$f_{\mathcal{S}}(\xi) = \sum_{S \in \mathcal{S}} \mathbf{e}(S\xi) = \sum_{G \in \mathcal{M}_n} v_G \mathbf{e}(G\xi),$$

where $v_G > 0$ iff $\mathrm{D}(G) = n - j$.

The method

By the orthogonality

$$\begin{aligned} I &= \int_{\mathbf{T}} f_{\mathcal{A}}(\xi) f_{\mathcal{B}}(\xi) f_{\mathcal{S}}(-\xi) \mathrm{d}\mu(\xi) \\ &= \int_{\mathbf{T}} \sum_{A \in \mathcal{A}} \sum_{B \in \mathcal{B}} \sum_{S \in \mathcal{S}} \mathbf{e}((A + B - S)\xi) \mathrm{d}\mu(\xi) \\ &= \int_{\mathbf{T}} \sum_{G \in \mathcal{M}_n} \sum_{H \in \mathcal{M}_n} u_G v_H \mathbf{e}((G - H)\xi) \mathrm{d}\mu(\xi) \\ &= \sum_{G \in \mathcal{M}_n} u_G v_G. \end{aligned}$$

If $I > 0$, then there is a $G \in \mathcal{A} + \mathcal{B}$ such that $\mathrm{D}(G) = n - j$.

Main part: investigate $f_{\mathcal{S}}$ on minor and major arcs.

Further problems

We have shown $\mathrm{D}(A+B) > n - c(\sigma)$ for $A \in \mathcal{A}, B \in \mathcal{B}$ if $(|\mathcal{A}||\mathcal{B}|)^{1/2} \geq q^{(6/7+\varepsilon)n}$.

- Smaller $\mathcal{A}, \mathcal{B}$?
  Let $z = \min\{\log|\mathcal{A}|/\log q, \log|\mathcal{B}|/\log q\}$, and estimate $\max \mathrm{D}(A+B)$ in terms of z.
- Multiplivative version: $\max \mathrm{D}(AB+1)$ for $A \in \mathcal{A}$, $B \in \mathcal{B}$ (ongoing).
- Is it true, that

$$\mathrm{D}\big((AB+1)(AC+1)(BC+1)\big) \to \infty$$

  as $\max\{\deg A, \deg B, \deg C\} \to \infty$?

  For integers, see Hernández and Luca (2003) or Corvaja and Zannier (2003).

Thank you!