Sum-Product Theory in Finite Fields

Derrick Hart
(Joint work with Alex Iosevich)

University of Missouri

Sums and Products

- Let $A \subset \mathbb{Z}$, finite, and define

$$A + A = \{a + a' : a, a' \in A\} \quad A \cdot A = \{aa' : a, a' \in A\}.$$

Sums and Products

- Let $A \subset \mathbb{Z}$, finite, and define

$$A + A = \{a + a' : a, a' \in A\} \quad A \cdot A = \{aa' : a, a' \in A\}.$$

- Can $|A + A|$ and $|A \cdot A|$ both be small?

Sums and Products

- Let $A \subset \mathbb{Z}$, finite, and define

$$A + A = \{a + a' : a, a' \in A\} \quad A \cdot A = \{aa' : a, a' \in A\}.$$

- Can $|A + A|$ and $|A \cdot A|$ both be small?
- Consider the examples

$$A = \{1, 2, \ldots, N\} \quad A = \{2, 2^2, \ldots, 2^N\}.$$

Sums and Products

- Let $A \subset \mathbb{Z}$, finite, and define

$$A + A = \{a + a' : a, a' \in A\} \quad A \cdot A = \{aa' : a, a' \in A\}.$$

- Can $|A + A|$ and $|A \cdot A|$ both be small?
- Consider the examples

$$A = \{1, 2, \dots, N\} \quad A = \{2, 2^2, \dots, 2^N\}.$$

- A conjecture due to Erdős and Szemeredi says that the answer is no.

Conjecture

With the notation above,

$$\max\{|A + A|, |A \cdot A|\} \gtrsim |A|^{2-\epsilon}.$$

Sums and Products

- The best known result in this direction is due to Solymosi who proved that
$$\max\{|A+A|, |A\cdot A|\} \gtrsim |A|^{\frac{14}{11}-\epsilon},$$
based partly on the idea to Elekes using the Szemeredi-Trotter Incidence Theorem, who proved the same estimate with a slightly worse exponent $\frac{5}{4}$.

Sums and Products

- The best known result in this direction is due to Solymosi who proved that

$$\max\{|A+A|, |A\cdot A|\} \gtrsim |A|^{\frac{14}{11}-\epsilon},$$

  based partly on the idea to Elekes using the Szemeredi-Trotter Incidence Theorem, who proved the same estimate with a slightly worse exponent $\frac{5}{4}$.

- Finite Field Case

Theorem (Bourgain-Katz-Tao)

If $A \subset \mathbb{Z}_p$, p a prime, and $p^\epsilon \lesssim |A| \lesssim p^{1-\epsilon}$, for some $\epsilon > 0$, then there exists $\delta > 0$ such that

$$\max\{|A+A|, |A\cdot A|\} \gtrsim |A|^{1+\delta}.$$

Explicit Bounds

- Using incidences between points and hyperbolae in the plane the author along with Alex Iosevich and Joszef Solymosi proved that if $A \subset \mathbb{F}_q$, a finite field with q elements, then

$$\max\{|A+A|, |A \cdot A|\} \gtrsim \min\{|A|^{\frac{3}{2}} q^{-\frac{1}{4}}, |A|^{\frac{2}{3}} q^{\frac{1}{3}}\}.$$

Explicit Bounds

- Using incidences between points and hyperbolae in the plane the author along with Alex Iosevich and Joszef Solymosi proved that if $A \subset \mathbb{F}_q$, a finite field with q elements, then

$$\max\{|A+A|, |A \cdot A|\} \gtrsim \min\{|A|^{\frac{3}{2}} q^{-\frac{1}{4}}, |A|^{\frac{2}{3}} q^{\frac{1}{3}}\}.$$

- This has been improved and generalized in many ways recently, The current best result is due to Garaev which is

$$\max\{|A+A|, |A \cdot A|\} \gtrsim \min\{|A|^2 q^{-\frac{1}{2}}, |A|^{\frac{1}{2}} q^{\frac{1}{2}}\}.$$

Explicit Bounds

- Using incidences between points and hyperbolae in the plane the author along with Alex Iosevich and Joszef Solymosi proved that if $A \subset \mathbb{F}_q$, a finite field with q elements, then

$$\max\{|A+A|, |A \cdot A|\} \gtrsim \min\{|A|^{\frac{3}{2}} q^{-\frac{1}{4}}, |A|^{\frac{2}{3}} q^{\frac{1}{3}}\}.$$

- This has been improved and generalized in many ways recently, The current best result is due to Garaev which is

$$\max\{|A+A|, |A \cdot A|\} \gtrsim \min\{|A|^{2} q^{-\frac{1}{2}}, |A|^{\frac{1}{2}} q^{\frac{1}{2}}\}.$$

- The above results yield non-trivial results only in the case that $|A| > q^{1/2}$ as one would expect with the existence of subfields of size $q^{1/2}$. In the case of prime fields however, one may get results in the lower range. The current best result due to Katz and Shen based on an improvement of a method of Garaev yields the for $|A| < q^{1/2}$,

$$\max\{|A+A|, |A \cdot A|\} \gtrsim |A|^{\frac{14}{13}-\epsilon}.$$

Sum-product basis in Finite Fields

- Let $\mathbb{F}_q$ be the finite field with q elements. How large does $A \subset \mathbb{F}_q$ need to be so that

$$\mathbb{F}_q = dA^2 = A \cdot A + A \cdot A \cdots + A \cdot A?$$

Sum-product basis in Finite Fields

- Let $\mathbb{F}_q$ be the finite field with q elements. How large does $A \subset \mathbb{F}_q$ need to be so that

$$\mathbb{F}_q = dA^2 = A \cdot A + A \cdot A \cdots + A \cdot A?$$

- Many results pertaining to this and related questions, under a variety of assumptions, have been published in recent years by Bourgain, Croot, Glibichuk, Konyagin, Shkredov, Tao, Vu and others. For $d \geq 8$ the problem was solved recently by Glibichuk extending earlier results of Glibichuk and Konyagin for prime fields.

Theorem (Glibichuk)

If $A \subset \mathbb{F}_q^*$, then

$$\mathbb{F}_q = 8A^2 \text{ if } |A| > \sqrt{2}q^{\frac{1}{2}}.$$

Short Sum-product basis

- What about when d is small?

Short Sum-product basis

- What about when d is small?
- Bourgain proved(specifically with d=3) using one-dimensional exponential sums that if q is prime and $A \subset \mathbb{F}_q^*$, then

$$\mathbb{F}_q = dA^2 \text{ if } |A| > q^{\frac{1}{2}+\frac{1}{2(d-1)}}.$$

Short Sum-product basis

- What about when d is small?
- Bourgain proved(specifically with d=3) using one-dimensional exponential sums that if q is prime and $A \subset \mathbb{F}_q^*$, then

$$\mathbb{F}_q = dA^2 \text{ if } |A| > q^{\frac{1}{2}+\frac{1}{2(d-1)}}.$$

- The author and Alex Iosevich recently proved the stronger result that if $A \subset \mathbb{F}_q^*$, then

$$\mathbb{F}_q^* \subset dA^2 \text{ if } |A| > q^{\frac{1}{2}+\frac{1}{2d}}, \quad \text{and} \quad |dA^2| > \frac{q}{2} \text{ if } |A| > q^{\frac{1}{2}+\frac{1}{2(2d-1)}}.$$

Sums and products-higher dimensional perspective

- Our idea is to take a higher dimensional perspective. Let $E \subset \mathbb{F}_q^d$, the d-dimensional vector space over $\mathbb{F}_q$. Define
$$\Pi(E) = \{x \cdot y : x, y \in E\}.$$
In this context we ask how large does E need to be to assure that $\Pi(E)$ is large?

Sums and products-higher dimensional perspective

- Our idea is to take a higher dimensional perspective. Let $E \subset \mathbb{F}_q^d$, the d-dimensional vector space over $\mathbb{F}_q$. Define

  $$\Pi(E) = \{x \cdot y : x, y \in E\}.$$

  In this context we ask how large does E need to be to assure that $\Pi(E)$ is large?
- Our main result is the following:

Theorem

Let $E \subset \mathbb{F}_q^d$. Then

$$\mathbb{F}_q^* \subset \Pi(E) \text{ if } |E| > q^{\frac{d+1}{2}},$$

and if E is a product set,

$$|\Pi(E)| > \frac{q}{2} \text{ if } |E| > q^{\frac{d^2}{2d-1}}.$$

Sums and products-higher dimensional perspective

- Our idea is to take a higher dimensional perspective. Let $E \subset \mathbb{F}_q^d$, the d-dimensional vector space over $\mathbb{F}_q$. Define

$$\Pi(E) = \{x \cdot y : x, y \in E\}.$$

  In this context we ask how large does E need to be to assure that $\Pi(E)$ is large?

- Our main result is the following:

Theorem

Let $E \subset \mathbb{F}_q^d$. Then

$$\mathbb{F}_q^* \subset \Pi(E) \text{ if } |E| > q^{\frac{d+1}{2}},$$

and if E is a product set,

$$|\Pi(E)| > \frac{q}{2} \text{ if } |E| > q^{\frac{d^2}{2d-1}}.$$

- Taking $E = A \times A \ldots \times A$ yields the arithmetic result.

Radon transforms make an appearance

- An inevitable way to study the dot product problem above is by considering the incidence function

$$\nu(t) = |\{(x, y) \in E \times E : x \cdot y = t\}|$$

Radon transforms make an appearance

- An inevitable way to study the dot product problem above is by considering the incidence function

$$\nu(t) = |\{(x, y) \in E \times E : x \cdot y = t\}|$$

- $$= \sum_{x \cdot y = t} E(x)E(y)$$

Radon transforms make an appearance

- An inevitable way to study the dot product problem above is by considering the incidence function

$$\nu(t) = |\{(x,y) \in E \times E : x \cdot y = t\}|$$

- $$= \sum_{x \cdot y = t} E(x)E(y)$$

- $$= \sum_{x} E(x)\mathcal{R}E(x),$$

Radon transforms make an appearance

- An inevitable way to study the dot product problem above is by considering the incidence function

$$\nu(t) = |\{(x, y) \in E \times E : x \cdot y = t\}|$$

- $$= \sum_{x \cdot y = t} E(x)E(y)$$

- $$= \sum_{x} E(x)\mathcal{R}E(x),$$

- where

$$\mathcal{R}E(x) = \sum_{x \cdot y = t} E(y),$$

  the Radon transform of E.

Why is it good to have a Radon transform around?

- In the Euclidean setting ($\mathbb{R}^d$, $d \geq 2$), consider

$$\mathcal{R}f(x) = \int_{x \cdot y = t} f(y)\psi(y)dy.$$

Why is it good to have a Radon transform around?

- In the Euclidean setting ($\mathbb{R}^d$, $d \geq 2$), consider

$$\mathcal{R}f(x) = \int_{x \cdot y = t} f(y)\psi(y)dy.$$

- In this case:

$$\mathcal{R} : L^2(\mathbb{R}^d) \to L^2_{\frac{d-1}{2}}(\mathbb{R}^d)$$

and a suitable analog holds in the finite field `setting`.

Resulting geometric incidence estimates

- Using the Radon transform, we establish the following incidence estimates:

Resulting geometric incidence estimates

- Using the Radon transform, we establish the following incidence estimates:
- $$\nu(t) = |E|^2 q^{-1} + R(t), \quad \text{where } |R(t)| \leq |E| q^{\frac{d-1}{2}},$$

Resulting geometric incidence estimates

- Using the Radon transform, we establish the following incidence estimates:
- $$\nu(t) = |E|^2 q^{-1} + R(t), \quad \text{where } |R(t)| \leq |E| q^{\frac{d-1}{2}},$$
- and
$$\sum_t \nu^2(t) = |E|^4 q^{-1} + |E| q^{2d-1} \sum_{k \neq \overrightarrow{0}} |\widehat{E}(k)|^2 |E \cap l_k|,$$

Resulting geometric incidence estimates

- Using the Radon transform, we establish the following incidence estimates:
- $$\nu(t) = |E|^2 q^{-1} + R(t), \quad \text{where } |R(t)| \le |E| q^{\frac{d-1}{2}},$$
- and
$$\sum_t \nu^2(t) = |E|^4 q^{-1} + |E| q^{2d-1} \sum_{k \neq \overrightarrow{0}} |\widehat{E}(k)|^2 |E \cap l_k|,$$
- where
$$l_k = \{tk : t \in \mathbb{F}_q\}, \text{ the line generated by } k.$$

Resulting geometric incidence estimates

- Using the Radon transform, we establish the following incidence estimates:

- $$\nu(t) = |E|^2 q^{-1} + R(t), \text{ where } |R(t)| \le |E| q^{\frac{d-1}{2}},$$

- and
$$\sum_t \nu^2(t) = |E|^4 q^{-1} + |E| q^{2d-1} \sum_{k \neq \overrightarrow{0}} |\widehat{E}(k)|^2 |E \cap l_k|,$$

- where
$$l_k = \{tk : t \in \mathbb{F}_q\}, \text{ the line generated by } k.$$

- Simple but important observation: if $E = A \times \ldots \times A$,
$$|E \cap l_k| \le |A|.$$

Open question

- It is possible to sharpen the positive proportion result. For example

Theorem (Shparlinski)

Let $A \subset F_q^*$ *then*

$$|A \cdot A + A| > \frac{q}{2}, \text{ for } |A| > q^{\frac{2}{3}}.$$

Open question

- It is possible to sharpen the positive proportion result. For example

Theorem (Shparlinski)

Let $A \subset F_q^*$ *then*

$$|A \cdot A + A| > \frac{q}{2}, \ \textit{for } |A| > q^{\frac{2}{3}}.$$

Question

Let $A \subset F_q^*$ *then does there exist an* $1/2 > \epsilon > 0$ *such that*

$$\mathbb{F}_q^* \subseteq A \cdot A + A, \ \textit{for } |A| > q^{1-\epsilon}.$$