Sum-product estimates in finite quasifields

Michael Tait

University of California-San Diego

mtait@math.ucsd.edu

September 26, 2015

Definitions

Let R an algebraic structure closed under "+" and "·", and let $A \subset R$. Define the *sum set* and *product set* of A to be

$$A + A = \{a + b : a, b \in A\}$$
$$A \cdot A = \{a \cdot b : a, b \in A\}$$

Warm up

Consider $\mathbb{Z}$ and let $A = \{1, 2, 5\}$.

$$A + A = \{2, 3, 4, 6, 7, 10\}$$
$$A \cdot A = \{1, 2, 4, 5, 10, 25\}$$

- When is $|A + A|$ small?
- When is $|A \cdot A|$ small?
- Can they both be small at the same time?

Previous work

When $A \subset \mathbb{Z}$, Erdős and Szemerédi showed that

$$\max\{|A+A|, |A \cdot A|\} = \Omega\left(|A|^{1+\varepsilon}\right).$$

On the other hand, if $\mathbb{F}$ is a field with subfield K, then $|K+K| = |K \cdot K| = |K|$.

When does a non-trivial sum-product estimate hold?

Previous work

Author	Setting	Notes
Erdős-Szemerédi	$\mathbb{Z}$	$1+\varepsilon$
Elekes	$\mathbb{Z}$	$5/4$
Solymosi	$\mathbb{C}$	$14/11 - o(1)$
Solymosi	$\mathbb{Z}$	$4/3 - o(1)$
Konyagin-Shkredov	$\mathbb{Z}$	$4/3 + 1/20598 - o(1)$
Bourgain-Katz-Tao	$\mathbb{F}_p$	$1 \ll \|A\| \ll p$
Garaev	$\mathbb{F}_p$	$\|A\| > p^{2/3}$
Hart-Iosevich-Solymosi	$\mathbb{F}_q$	$\|A\| \gg q^{1/2}$
Vu	$\mathbb{F}_q$	more general
Tao	Ring	zero divisors/subring

Conjecture: If $A \subset \mathbb{Z}$ then $\max\{|A+A|, |A \cdot A| \geq |A|^{2-o(1)}$.

Szemerédi-Trotter Theorem

Some of these results were proved using the Szemerédi-Trotter Theorem.

Theorem

Given n points and m lines in the plane, they determine at most

$$O\left(n^{2/3}m^{2/3} + n + m\right)$$

incidences.

We prove a Szemerédi-Trotter Theorem set in a quasifield and use it to deduce a sum-product estimate.

Quasifields

A quasifield $(Q, +\cdot)$ satisfies

1. Q is a group under addition.
2. Q is a loop under multiplication. i.e. the multiplication table of Q is a Latin square.
3. Left distributivity: $a \cdot (b + c) = a \cdot b + a \cdot c$.
4. $a \cdot x = b \cdot x + c$ has exactly one solution for $a, b, c \in Q$.

A quasifield is like a field except that multiplication need not be associative or commutative, and Q may not satisfy right-distributivity.

Projective planes

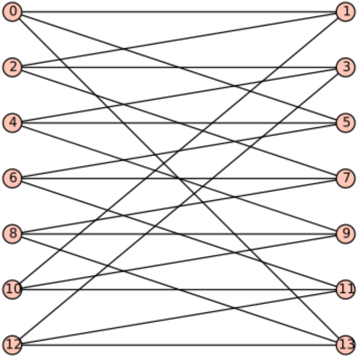
To prove a Szemerédi-Trotter theorem in a quasifield, we coordinatize a projective plane Π.

$$\mathcal{P} = \{(x,y) : x, y \in Q\} \cup \{(x) : x \in Q\} \cup \{(\infty)\}$$
$$\mathcal{L} = \{[m,b] : m, k \in Q\} \cup \{[m] : m \in Q\} \cup \{[\infty]\}$$

Incidence is defined by the rules

- $(x,y) \sim [m,b]$ iff $m \cdot x + y = b$
- $(x,y) \sim [b]$ iff $x = b$
- $(x) \sim [m,b]$ iff $x = m$
- $(x) \sim \infty$ and $(\infty) \sim [b]$
- $(\infty) \sim [\infty]$

Pseudorandomness



Bipartite incidence graphs of projective planes are pseudorandom.

Szemerédi-Trotter in quasifields

We want to prove a variant of the Szemerédi-Trotter incidence theorem in Q. What do we mean by “lines” in a quasifield? For $a, b \in Q$

$$l(a,b) = \{(x,y) \in Q^2 : y = b \cdot x + a\}.$$

Theorem (Pham, MT, Timmons, Vinh)

Let Q be a quasifield of order q. Let P be a set of points in Q^2 and L be a set of lines in Q^2, then

$$|\{(p,l) \in P \times L : p \in l\}| \leq \frac{|P||L|}{q} + q^{1/2}\sqrt{|P||L|}.$$

Szemerédi-Trotter in quasifields

Proof: Let $R \subset Q^2$ and $L = \{l(a,b) : a, b \in R\}$ be a set of lines. Let $P \subset Q^2$ be a set of points. (p_1, p_2) is on $l(a,b)$ if and only if $p_2 = b \cdot p_1 + a$.
This is equivalent to $(p_1, -p_2) \sim [b, -a]$ in Π. Let

$$S = \{(p_1, -p_2) : (p_1, p_2) \in P\}$$
$$T = \{[b, -a] : (a, b) \in R\}$$

Then the number of edges between S and T in the Levi graph of Π exactly counts the number of point-line incidences between P and L. Apply the expander-mixing lemma.

Sum-product estimates in Q

Let $A \subset Q$. We define a set of points and lines that measure $|A + A|$ and $|A \cdot A|$ and then apply our Szemerédi-Trotter theorem.

$$P = (A + A) \times (A \cdot A)$$
$$L = \{l(-a \cdot b, a) : a, b \in A\}$$

Recall $l(c, d) = \{(x, y) : y = d \cdot x + c\}$. For any $a, b, c \in A$,

the point $(c + b, a \cdot c) \in P$ is on the line $l(-a \cdot b, a) \in L$.

$$a \cdot c = a \cdot (c + b) - a \cdot b.$$

$|A|^3$ incidences defined by $|A|^2$ lines and $|A + A||A \cdot A|$ points.

Sum-product estimates in Q

Theorem (Pham, MT, Timmons, Vinh)

Let Q be a quasifield of order Q. Then if $q^{1/2} \ll |A| \ll q^{2/3}$,

$$\max\{|A+A|, |A \cdot A|\} = \Omega\left(\frac{|A|^2}{q^{1/2}}\right).$$

If $q^{2/3} \leq |A| \ll q$, *then*

$$\max\{|A+A|, |A \cdot A|\} = \Omega\left((q|A|)^{1/2}\right)$$

Open Questions

- Erdős and Szemerédi conjecture: for $A \subset \mathbb{Z}$, is $\max\{|A+A|, |A \cdot A|\} = |A|^{2-o(1)}$?

- The spectral method can only give non-trivial estimates when $|A| \gg q^{1/2}$. It is probably true that if $A \subset Q$ with $1 \ll |A| \ll q$ and A is not "close to a sub-quasifield", then $\max\{|A+A|, |A \cdot A|\} \geq |A|^{1+\varepsilon}$.