Szemerédi-Trotter type theorem and sum-product estimate in finite fields

Le Anh Vinh
Mathematics Department
Harvard University
Cambridge, MA 02138, US
vinh@math.harvard.edu

February 2, 2008

Abstract
We study a Szemerédi-Trotter type theorem in finite fields. We then use this theorem to obtain an improved sum-product estimate in finite fields.

1 Introduction
Let $A$ be a non-empty subset of a finite field $F_q$. We consider the sum set
\[ A + A := \{a + b : a, b \in A\} \]
and the product set
\[ A.A := \{a.b : a, b \in A\}. \]

Let $|A|$ denote the cardinality of $A$. Bourgain, Katz and Tao (\cite{4}) showed, using an argument of Edgar and Miller (\cite{5}), that when $1 \ll |A| \ll q$ then
\[ \max(|A + A|, |A.A|) \gg |A|; \]
this improves the easy bound $|A + A|, |A.A| \geq |A|$. The precise statement of the sum-product estimate is as follows.

Theorem 1 (\cite{4}) Let $A$ be a subset of $F_q$ such that
\[ q^\delta < |A| < q^{1-\delta} \]
for some $\delta > 0$. Then one has a bound of the form
\[ \max(|A + A|, |A.A|) \geq c(\delta)|A|^{1+\epsilon} \]
for some $\epsilon = \epsilon(\delta) > 0$. 

Using Theorem 1, Bourgain, Katz and Tao can prove a theorem of Szemerédi-Trotter type in two-dimensional finite field geometries. Roughly speaking, this theorem asserts that if we are in the finite plane $F_q^2$ and one has $N$ lines and $N$ points in that plane for some $1 \ll N \ll q^2$, then there are at most $O(N^{3/2 - \epsilon})$ incidences; this improves the standard bound of $O(N^{3/2})$ obtained from extremal graph theory. The precise statement of the theorem is as follows.

**Theorem 2** ([4]) Let $P$ be a collection of points and $L$ be a collection of lines in $F^2$. For any $0 < \alpha < 2$, if $|P|, |L| \leq N = q^\alpha$ then we have

$$|\{(p, l) \in P \times L : p \in l\}| \leq CN^{3/2 - \epsilon},$$

for some $\epsilon = \epsilon(\alpha) > 0$ depending only on the exponent $\alpha$.

The relationship between $\epsilon$ and $\delta$ in Theorem 1 and the relationship between $\alpha$ and $\epsilon$ in Theorem 2 however are difficult to determine.

In this paper we shall proceed in an opposite direction. We will first prove a theorem of Szemerédi-Trotter type about the number of incidences between points and lines in finite field geometries. We then apply this result to obtain an improved sum-product estimate. Our first result is the following.

**Theorem 3** Let $P$ be a collection of points and $L$ be a collection of lines in $F_q^2$. Then we have

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

In the spirit of Bourgain-Katz-Tao’s result, we obtain a reasonably good estimate when $1 < \alpha < 2$.

**Corollary 1** Let $P$ be a collection of points and $L$ be a collection of lines in $F_q^2$. Suppose that $|P|, |L| \leq N = q^\alpha$ with $1 + \epsilon \leq \alpha \leq 2 - \epsilon$ for some $\epsilon > 0$. Then we have

$$|\{(p, l) \in P \times L : p \in l\}| \leq 2N^{3/2 - \frac{\epsilon}{4}}. \quad (2)$$

We shall use the incidence bound in Theorem 3 to obtain an improved sum-product estimate.

**Theorem 4** (sum-product estimate) Let $A \subset F_q$ with $q$ is an odd prime power. Suppose that

$$|A + A| = m, |A.A| = n.$$

Then

$$|A|^2 \leq \frac{mn|A|}{q} + q^{1/2} \sqrt{mn}.$$

In particular, we have

$$\max(|A + A|, |A.A|) \geq \frac{2|A|^2}{q^{1/2} + \sqrt{q + \frac{4|A|^3}{q}}} \quad (3)$$

In analogy with the statement of Corollary 1 above, we note the following consequence of Theorem 4.

**Corollary 2** Let $A \subset F_q$ with $q$ is an odd prime power.

1. Suppose that $q^{1/2} \ll |A| \leq q^{2/3}$. Then
   \[
   \max(|A + A|, |A.A|) \geq c\frac{|A|^2}{q^{1/2}}.
   \]

2. Suppose that $q^{2/3} \leq |A| \ll q$. Then
   \[
   \max(|A + A|, |A.A|) \geq c(q|A|)^{1/2}.
   \]

Note that, the bound in Theorem 4 is stronger than ones established in Theorem 1.1 in [7].

We also call the reader’s attention to the fact that the application of the spectral method from graph theory in sum-product estimates was independently used by Vu in [16]. The bound in Corollary 2 is stronger than ones in Remark 1.4 from [16] (which is also implicit from Theorem 1.1 in [7]).

## 2 Incidences: Proofs of Theorem 3 and Corollary 1

We can embed the space $F_q^2$ into $PF_q^3$ by identifying $(x, y)$ with the equivalence class of $(x, y, 1)$. Any line in $F_q^2$ also can be represented uniquely as an equivalence class in $PF_q^3$ of some non-zero element $h \in F_q^2$. For each $x \in F_q^3$, we denote $[x]$ the equivalence class of $x$ in $GF_q^3$. Let $G_q$ denote the graph whose vertices are the points of $PF_q^3$, where two vertices $[x]$ and $[y]$ are connected if and only if
\[
\langle x, y \rangle = x_1y_1 + x_2y_2 + x_3y_3 = 0.
\]
That is the points represented by $[x]$ and $[y]$ lie on the lines represented by $[y]$ and $[x]$, respectively.

It is well-known that $G_q$ has $n = q^2 + q + 1$ vertices and $G_q$ is a $(q + 1)$-regular graph. Since the equation $x_1^2 + x_2^2 + x_3^2 = 0$ over $F_q$ has exactly $q^2 - 1$ non-zero solutions so the number of vertices of $G$ with loops is $d = q + 1$. The eigenvalues of $G$ are easy to compute. Let $A$ be the adjacency matrix of $G$. Since two lines in $PF_q^3$ intersect at exactly one point, we have $A^2 = AA^T = J + (d - 1)I = J + qI$ where $J$ is the $n \times n$ all 1-s matrix and $I$ is the $n \times n$ identity matrix. Thus the largest eigenvalue of $A^2$ is $d^2$ and all other eigenvalues are $d - 1 = q$. This implies that all but the largest eigenvalues of $G_q$ are $\sqrt{q}$.

It is well-known that if a $k$-regular graph on $n$ vertices with the absolute value of each of its eigenvalues but the largest one is at most $\lambda$ and if $\lambda \ll d$ then this graph behaves similarly as a random graph $G_{n,k/n}$. Presicely, we have the following result (see Corollary 9.2.5 in [2]).
Lemma 1 Let $G$ be a $k$-regular graph on $n$ vertices (with loops allowed). Suppose that all eigenvalues of $G$ except the largest one are at most $\lambda$. Then for every set of vertices $B$ and $C$ of $G$, we have

$$|e(B, C) - \frac{k}{n}|B||C| \leq \lambda\sqrt{|B||C|},$$

where $e(B, C)$ is the number of ordered pairs $(u, v)$ where $u \in B, v \in C$ and $uv$ is an edge of $G$.

Let $B$ be the set of vertices of $G$ that represent the collection $P$ of points in $F^2_q$ and $C$ be the set of vertices of $G$ that represent the collection $L$ of lines in $F^2_q$. From (4), we have

$$|\{(p, h) \in P \times L : p \in h\}| = e(B, C) \leq \frac{q + 1}{q^2 + q + 1}|B||C| + \lambda\sqrt{|B||C|} \leq \frac{|P||L|}{q} + q^{1/2}\sqrt{|P||L|}.$$

This concludes the proof of Theorem 3.

If $\alpha \leq 2 - \varepsilon$ then

$$\frac{|P||L|}{q} \leq \frac{N^2}{q} \leq N^{\frac{3}{2} - \frac{\varepsilon}{4}}.$$

If $\alpha \geq 1 + \varepsilon$ then

$$q^{1/2}\sqrt{|P||L|} \leq q^{1/2}N \leq N^{\frac{3}{2} - \frac{\varepsilon}{4}}.$$

Corollary 1 are immediate from (5), (6) and Theorem 3.

Note that we also have an analog of Theorem 3 in higher dimension.

Theorem 5 Let $P$ be a collection of points in $F^d_q$ and $H$ be a collection of hyperplanes in $F^d_q$ with $d \geq 2$. Then we have

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

The proof of this theorem is similar to the proof of Theorem 3 and is left for the readers. Note that the analog of Theorem 5 for the case $P \equiv L$ (in $PF^d_q$) are obtained by Alon and Krivelevich ([1]) via a similar approach and by Hart, Iosevich, Koh and Rudnev ([9]) via Fourier analysis. By modifying the proofs of Theorem 2.1 in [9] and Lemma 2.2 in [1] slightly, we obtain Theorem 5.
3 Sum-product estimates: Proofs of Theorem 4 and Corollary 2

Elekes ([6]) observed that there is a connection between the incidence problem and the sum-product problem. The statement and the proof here follow the presentation in [4].

Lemma 2 ([6]) Let $A$ be a subset of $F_q$. Then there is a collection of points $P$ and lines $L$ with $|P| = |A + A| |A.A|$ and $|L| = |A|^2$ which has at least $|A|^3$ incidences.

Proof Take $P = (A + A) \times (A.A)$, and let $L$ be the collection of all lines of form $l(a, b) := \{(x, y) : y = b(x - a)\}$ where $a, b \in A$. The claim follows since $(a + c, bc) \in P$ is incident to $l(a, b)$ whenever $a, b, c \in A$.

□

Theorem 4 follows from Theorem 3 and Lemma 2.

Proof (of Theorem 4) Let $P$ and $L$ be collections of points and lines as in the proof of Lemma 1. Then from Theorem 3, we have

$$|A|^3 \leq \frac{mn|A|^2}{q} + q^{1/2}|A|\sqrt{mn}.$$  

This implies that

$$|A|^2 \leq \frac{mn|A|}{q} + q^{1/2}\sqrt{mn}.$$  

Let $x = \max(|A + A|, |A.A|)$, we have

$$|A|x^2 + q^{3/2}x - q|A|^2 \geq 0.$$  

Solving this inequality gives us the desired lower bound for $x$, concluding the proof of the theorem.

□

If $q^{1/2} \ll |A| \ll q^{2/3}$. Then

$$q^{1/2} + \sqrt{q + \frac{4|A|^3}{q}} = O(q^{1/2}).$$  

If $q^{2/3} \ll |A| \ll q$. Then

$$q^{1/2} + \sqrt{q + \frac{4|A|^3}{q}} = O(\sqrt{|A|^3/q}).$$  

Corollary 2 is immediate from (9), (10) and Theorem 4.

5
References

[1] N. Alon, M. Krivelevich, Constructive bounds for a Ramsey-type problems, *Graphs and Combinatorics* **13** (1997), 217-225.

[2] N. Alon, J.H. Spencer, *The Probabilistic Method*, 2nd edition, Wiley-Interscience, 2000.

[3] J. Bourgain, Hausdorff dimension and distance sets, *Israel Journal of Mathematics* **87** (1994), 1993-201.

[4] J. Bourgain, N. Katz, T. Tao, A sum-product estimate in finite fields, and applications, *Geom. Funct. Anal.* **14** (2004), 27-57.

[5] G.A. Edgar, C. Miller, Borel subrings of the reals, *Proceedings of American Mathematical Society* **131** (2003), 1121-1129.

[6] G. Elekes, On the number of sums and products, *Acta Arithmetica* **81** (1997), 365-367.

[7] D. Hart, A. Iosevich, J. Solymosi, Sum-product estimates in finite fields via Kloosterman sums, *International Mathematics Research Notices* (to appear).

[8] D. Hart, A. Iosevich, Sums and products in finite fields: an integral geometric viewpoint, preprint, 2007.

[9] D. Hart, A. Iosevich, D. Koh and M. Rudnev, Averages over hyperplanes, sum-product theory in vector spaces over finite fields and the Erdös-Falconer distance conjecture, preprint, 2007.

[10] A. Iosevich, D. Koh, Erdös-Falconer distance problem, exponential sums, and Fourier analytic approach to incidence theorems in vector spaces over finite fields, preprint.

[11] A. Iosevich, M. Rudnev, Erdös distance problem in vector spaces over finite fields, *Transactions of the American Mathematical Society* **359** (12) (2007), 6127-6142.

[12] T. Tao, Finite field analogues of Erdös, Falconer, and Furstenberg problems, preprint.

[13] L.A. Vinh, Some coloring problems for unit-quadrance graphs, *The proceedings of Australian Workshop on Combinatorial Algorithms*, 2006, 361-367.

[14] L.A. Vinh and D.P.Dung, Explicit tough Ramsey graphs, preprint, 2007.

[15] L.A. Vinh, Explicit Ramsey graphs and Erdös distance problem over finite Euclidean and non-Euclidean spaces, submitted.

[16] V. Vu, Sum-Product estimates via directed expanders, preprint, 2007.