FINITE FIELDS AND APPLICATIONS
Additive Combinatorics in finite fields (3 lectures)

Ana Zumalacárregui
a.zumalacarregui@unsw.edu.au

November 30, 2015

Contents

**

1 Operations on sets

Let $A \subseteq \mathbb{F}$ a finite non-empty subset of a field (ring or group). We define the sumset and the product set as

$$A + A = \{a + a' \in \mathbb{F} : a, a' \in A\},$$
$$A \cdot A = \{a \cdot a' \in \mathbb{F} : a, a' \in A\},$$

similarly one can define the sets $A - A$ or $A^{-1} + A^{-1}$.

In general, for any rational function $H \in \mathbb{F}(x_1, \dots, x_n)$ and finite sets $A_1, \dots, A_n \subseteq \mathbb{F}$ we can consider the set:

$$H(A_1, \dots, A_n) = \{H(a_1, \dots, a_n) \in \mathbb{F} : a_1 \in A_1, \dots, a_n \in A_n\} \subseteq \mathbb{F}.$$

Remark 1. *Observe that generally speaking $A(A+1) \neq A^2 + A$, since for $a \neq b$ elements in A, the element $a(b+1)$ might not belong to $A^2 + A$ as well as $a^2 + b$ might not belong to $A(A+1)$.*

One of the major interest in Additive Combinatorics is to understand how the cardinality of these operation sets is connected to underlying structure in the original sets.

We will focus in this lectures on the so called Sum-product dichotomy, which compares the additive and multiplicative structure of sets. Before discussing the finite field case, we should first consider the integral case[1]: where both the sumset and the product set grow between linearly and quadratically in the size of the set.

[1]Observe that the discussion for sets of integers is in fact the same as the real case one, since all arguments can be extended to $\mathbb{R}$ and in fact the integral case should be understood as a simple restriction from the real one.

Proposition 1.1. *Let $A \subseteq \mathbb{Z}$ a non-empty finite set. Then*

$$2|A| - 1 \leq |A + A|, |A \cdot A| \leq \frac{|A|(|A| + 1)}{2}$$

Proof. For the upper bound, observe that all possible sums (resp. products) are at most the number of pairs $\{a, a'\}$ with elements $a, a' \in A$. There are exactly $\binom{|A|}{2} + |A|$ of those pairs (coming from $a \neq a'$ and $a = a'$).

For the lower bound we will focus on $A + A$, since $A \cdot A$ is analogous. Let

$$A = \{a_i, \ldots, a_k\} \quad \text{with} \quad a_1 < a_2 < \cdots < a_k.$$

Then, we have $2|A| - 1$ distinct sums

$$a_1 + a_1 < a_1 + a_2 < a_1 + a_3 < \cdots < a_1 + a_k < a_2 + a_k < \cdots < a_{k-1} + a_k < a_k + a_k,$$

which are elements from $A + A$, which concludes the proof. □

Corollary 1.2. *Let A be a finite nonempty subset of integers, then $|A + A| = 2|A| - 1$ if and only if A is an arithmetic progression and $|A \cdot A| = 2|A| - 1$ if and only if A is a geometric progression.*

Proof. If $|A + A| = 2|A| - 1$ this implies that the elements in the chain are all the possible ones. Thus, we can construct the following chains

$$\begin{aligned} &a_1 + a_1 < a_1 + a_2 < a_1 + a_3 < a_1 + a_4 < \cdots < a_1 + a_k \ < a_2 + a_k < \cdots \\ &a_1 + a_1 < a_2 + a_1 < a_2 + a_2 < a_2 + a_3 < \cdots < a_2 + a_{k-1} < a_2 + a_k < \cdots \end{aligned}$$

of length $2|A| - 1$. Since element by element, both chains must coincide, in particular we have that for every $i = 1, \ldots, k - 1$

$$a_2 + a_i = a_1 + a_{i+1}$$

which implies in particular that

$$a_2 - a_1 = a_3 - a_2 = a_4 - a_3 = \cdots = a_k - a_{k-1} = d$$

or in other words: A is an arithmetic progression of difference d. The same argument shows that if $|A \cdot A| = 2|A| - 1$ then for every $i = 1, \ldots, k - 1$

$$a_2 \cdot a_i = a_1 \cdot a_{i+1}$$

which implies that $a_2/a_1 = a_3/a_2 = a_4/a_3 = \cdots = a_k/a_{k-1} = r$ and A is a geometric progression of ration r. □

In conclusion both the sumset and product set grow slowly, i.e. linearly in the size of A, only when the set is very structured but, what should we expect for a general subset?

Example 1. *Let $A = \{1, 2, 6, 12, 15\}$ be a set of integers. For this particular set A the quantities in Proposition 1.1 are*

$$9 \leq |A + A|, |A \cdot A| \leq 15. \tag{1}$$

In particular, we have

$$\begin{aligned} A + A &= \{2, 3, 4, 7, 8, 12, 13, 14, 16, 17, 18, 21, 24, 27, 30\}, \\ A \cdot A &= \{1, 2, 4, 6, 12, 15, 24, 30, 36, 72, 90, 144, 180, 225\}. \end{aligned}$$

Thus $|A + A| = 15$ and $|A \cdot A| = 14$. In both cases this quantities are closer to the upper bound in (1).

This is in fact the expected behaviour for a random set of integers: both the sumset and the product set grow considerably fast, i.e. quadratically in the size of A.

2 Sum-product theorem and its variations

Observe that if $A = \{a \cdot r^s : 1 \leq s \leq k\}$ is a geometric progression it follows from Corollary 1.2 that the size of $|A \cdot A|$ is minimal. Nevertheless, if we consider the sumset $|A + A|$ it turns out that all sums are different: since for every element x in the sumset there exists a unique representation of the form

$$x = a \cdot r^s + a \cdot r^t = a \cdot r^s(1 + r^{t-s}),$$

with $t \geq s$. This implies that the sumset is maximal and thus $|A + A| = |A|(|A| + 1)/2$.

We will discuss later how big the product set of an arithmetic progression might be (see Example 2).

One might wonder, is it possible to construct a set whose sumset and product set are small? Could a set behave both as an arithmetic progression and as a geometric progression at the same time?

Over $\mathbb{R}$, this question was first studied by Erdős and Szemerédi who showed in 1983 the following result, known as the Sum-Product Theorem.

Theorem 2.1 (Erdős-Szemerédi)**.** *Let $A \subseteq \mathbb{R}$ be a finite non-empty set then, for some fixed $\delta > 0$,*

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

It was conjectured by Erdős and Szemerédi that one can take δ arbitrarily close to 1 in Theorem 2.1. Many authors have worked on this problem and obtained different values for δ: Nathanson (1997, $\delta = 1/31$), Ford (1998, $\delta = 1/15$) or Elekes (1997, $\delta = 1/4$).

The best known bound for δ is due to Solymosi. In fact he showed in 2008 something rather stronger.

Theorem 2.2 (Solymosi)**.** *Let $A \subseteq \mathbb{R}$ be a finite non-empty set then*

$$|A + A|^2|A \cdot A| \geq \frac{|A|^4}{\log |A|}.$$

Note that it follows from this result that one could take any $\delta < 1/3$, improving previous results.

Corollary 2.3. *Let $A \subseteq \mathbb{R}$ be a finite non-empty set. If $|A + A| \ll |A|$ then*

$$|A \cdot A| \gg |A|^{2-o(1)}.$$

Proof. It follows from Theorem 2.2 that

$$|A \cdot A| \geq \frac{|A|^2}{|A + A|^2} \cdot \frac{|A|^2}{\log |A|} \gg \frac{|A|^2}{\log |A|}.$$

□

Example 2. *If $A = \{1, 2, \ldots, n\}$ then clearly $|A + A| = 2n - 1$, so it follows from Solymosi's result that $|A \cdot A| \gg |A|^{2-o(1)}$. One could be tempted to think that this case might be the analogous to the geometric progression case, discussed at the beginning of this section, and conclude that $|A \cdot A| \gg |A|^2$.*

Nevertheless, this case is way more delicate and the previous affirmation is not correct. As it turns out, the study of $|A \cdot A|$ in this case is related to the famous Erdős multiplication table problem. In 1955 Erdős [4] already showed that $|A \cdot A| = o(n^2)$ and, even if the asymptotic for this quantity is still unknown, the best known bound is due to Ford [5], who showed that if $A = \{1, \ldots, n\}$

$$|A \cdot A| \ll \frac{n}{(\log n)^c (\log \log n)^{3/2}},$$

for some explicit constant c, which in particular implies that the $o(1)$ term in Corollary 2.3 is necessary.

Remark 2. *Is it true that if $|A \cdot A| \ll |A|$ implies that $|A + A| \gg |A|^{2-o(1)}$? This problem remains open.*

2.1 Sum-product in prime fields

In 2003, Bourgain-Katz-Tao obtained the analogous to Erdős-Szemerédi sum-product theorem for sets in prime fields and derived interesting incidence results in finite fields (see Section 4).

Theorem 2.4 (Bourgain-Katz-Tao [1]). *For any $\epsilon > 0$, there exists $\delta = \delta(\epsilon) > 0$ such that if $p^\epsilon \leq |A| \leq p^{1-\epsilon}$ then*

$$\max\left\{|A+A|, |A\cdot A|\right\} \gg |A|^{1+\delta}.$$

Bourgain, Glibichuk and Konyagin showed in 2005 that the hypothesis $|A| \geq p^\epsilon$ can be omitted and the same result still holds.

One could be tempted of generalising Edős-Szemerédi Conjecture in the case of prime fields, but in fact one cannot expect to get as far as $|A|^{2-o(1)}$ in this case since, provided that we are in a finite setting, it is clear that for large sets there might not be enough space to grow at this rate.

We will now discuss the limitations of what can be true in this setting, even if the set is not that *large*.

Remark 3. *Let H be a multiplicative subgroup of $\mathbb{F}_p^\times$ of order $|H| \sim p^{3/4+o(1)}$ for a suitable prime p. It follows from the pigeon hole principle that, for some $m \in \mathbb{F}_p$ the set*

$$A = H \cap \{m+1, \cdots, m+\lfloor p^{3/4}\rfloor\}$$

satisfies

$$|A| \sim \frac{|H|p^{3/4}}{p} \sim p^{1/2+o(1)}.$$

Observe that, for such a set A we have that

$$\max\{|A+A|, |A\cdot A|\} \leq p^{3/4+o(1)},$$

since $A\cdot A \subset H$ and $A+A \subseteq \{m+2, \cdots, m+\lfloor 2p^{3/4}\rfloor\}$ by definition.

In fact, for every integer k

$$\max\left\{\left|k\cdot A\right|, \left|A^{(k)}\right|\right\} \leq p^{3/4+o(1)},$$

where $k\cdot A = A+\cdots+A$ and $A^{(k)} = A\cdots A$ denote the k-fold sum and product of A.

In particular, this implies that we could not expect to obtain anything better that

$$\max\{|A+A|, |A\cdot A|\} \geq |A|^{3/2+o(1)}.$$

Many authors have worked on this problem since Bourgain-Katz-Tao obtained their result: Bourgain, Chang, Garaev, Rudnev... The current status for the sum-product problem in prime fields could be summarized as follows:

Theorem 2.5. *Let p be a prime. For any non-empty set $A \subseteq \mathbb{F}_p$ we have*

$$\max\left\{|A+A|, |A\cdot A|\right\} \gg \begin{cases} |A|^{12/11+o(1)} & \text{if} \quad |A| \leq p^{1/2}, \\ |A|^{7/6}p^{-1/24+o(1)} & \text{if} \quad p^{1/2} \leq |A| \leq p^{35/68}, \\ |A|^{10/11}p^{1/11+o(1)} & \text{if} \quad p^{35/69} \leq |A| \leq p^{13/24}, \\ |A|^2 p^{-1/2} & \text{if} \quad p^{13/24} \leq |A| \leq p^{2/3}, \\ |A|^{1/2}p^{1/2} & \text{if} \quad p^{2/3} \leq |A| \leq p. \end{cases}$$

The last bound is tight and this is the only range where a tight bound is known.

2.2 Sum-product in finite fields

In general finite fields it appears a natural restriction in order to obtain a result analogous to Theorem 2.4: $\mathbb{F}_q$ contains subfields.

Remark 4. *If $H \subsetneq \mathbb{F}_q$ is a proper subfield of $\mathbb{F}_q$, then both the sumset and product set satisfy*

$$H + H = H \cdot H = H,$$

and similarly if A is contained in a proper subfield H then $A + A, A \cdot A \subseteq H$. Thus, we cannot expect for general finite fields a bound of the form $\max\{|A + A|, |A \cdot A|\} \geq |A|^{1+\delta}$ for every $|A| < q^{1-\epsilon}$ and some positive $\delta = \delta(\epsilon)$.

The case when $|A| \sim \sqrt{q}$ appears somewhat borderline, at least in the way in which the sum-product problem has been studied. We will mostly refer here to the case $|A| > q^{1/2}$, the *large set* case. Observe that the largest possible proper subfield of $\mathbb{F}_q$ has at most $q^{1/2}$ elements, therefore large sets are never subsets of proper subfields.

In 2007 Garaev [6], by means of exponential sums, proved the following result for general finite fields.

Theorem 2.6 (Garaev)**.** *Let $A \subseteq \mathbb{F}_q$, where q is a prime power,*

$$\max\{|A + A|, |A \cdot A|\} \gg \min\left\{\sqrt{|A|q}, \frac{|A|^2}{q^{1/2}}\right\}.$$

The previous result is optimal for $|A| > q^{2/3}$ and worse than trivial if $|A| \leq q^{1/2}$. The same result was re-derived by Vinh [8] from a very general incidence theorem which will be discussed in Section 4.

3 Applications to Waring problem in finite fields

Let $\gamma(k, q)$ denote the smallest integer s such that sums of kth powers of s elements in $\mathbb{F}_q$ represent every element in $\mathbb{F}_q$. That is, for every $x \in \mathbb{F}_q$ there exists at least one solution to

$$x = g_1^k + \cdots + g_s^k, \quad \text{with} \quad g_1, \ldots, g_s \in \mathbb{F}_q.$$

Remark 5. *If the set of kth powers $H_k := \{x^k : x \in \mathbb{F}_q\}$ is included in an additive nontrivial subgroup H of $\mathbb{F}_q$, then the quantity $\gamma(k, q)$ does not exist, since*

$$H_k + \overset{s}{\cdots} + H_k \subseteq H,$$

for every integer s.

The previous remark could be summarised in the following result.

Proposition 3.1. *Let $q = p^n$, for some prime p. The quantity $\gamma(k, q)$ exists if and only if $(p^n - 1)/(p^d - 1) \nmid k$ for every $d \mid n$, $1 \leq d < n$.*

Proof. Left as an exercise for the reader.

Theorem 3.2 (Cauchy)**.** *If $\gamma(k, q)$ exists, then*

$$\gamma(k, q) \leq k.$$

With character sums we were able to show that:

Theorem 3.3. *If $q > (k - 1)^2$, then*

$$\gamma(k, q) \leq \left\lfloor \frac{\log q}{\log q - \log(k - 1)} + 1 \right\rfloor.$$

(We did not have time to prove this result in class in full detail, but it will be included in the notes for character sums.)

In fact, for small values of k, the best known bounds [9] are of order $\log k$.

Theorem 3.4. *If γ exists and $q > k^2$, then*

$$\gamma(k,q) \leq \lfloor 32 \log k \rfloor + 1.$$

Nevertheless, the classical methods with character sums are only effective if the set A_k of kth powers is *large* (of order at least $q^{1/2+\epsilon}$).

In 2007 Cochrane and Pinner [2] proved the so called Heilbronn conjecture for prime fields exploiting the known sum-product estimates in finite fields. In 2009, Cipra generalised their result to general finite fields, but let me sketch the following result obtained in prime fields.

Theorem 3.5. *If $\gamma(k,p)$ exists, then*

$$\gamma(k,p) \ll \sqrt{k}.$$

Sketch of the proof. For a fixed suitable k, if H_k is large, namely $|H_k| \gg p^{1/2+\epsilon}$ for some positive ϵ, it is easy to check that Theorem 3.4 applies since $k = k_1 d$ with $(d, p-1) = 1$ and k_1 is small.

Let us denote by

$$A_s = \{x_1^k + \cdots + x_s^k : x_i \in \mathbb{F}_p\} = H_k + \overset{s}{\cdots} + H_k.$$

Note that $A_s + A_s = A_{2s}$ and $A_s \cdot A_s = A_{s^2}$ and it follows from Theorem 2.2 that at least one of them grows in size.

We can start with some s and iterate the process. In a finite number of steps we will reach $|A_d| > p^{1/2+\epsilon}$ and switch to character sum techniques. □

4 Connections to Szemerédi-Trotter in finite fields

We will now discuss the relation between some incidence results in discrete geometry and the sum-product theorems we have previously discussed. The first time these two problems were connected was in [3], where Elekes exploited the well known Szemerédi-Trotter theorem to obtain a bound for the sum-product problem.

In this section we will discuss Elekes' ideas in $\mathbb{R}$ and compare them with the analogous for finite fields.

4.1 Incidence theorems

Let P be a set of points in $\mathbb{R}^2$ and L a set of lines

$$\ell(a,b) = \{(x,y) \in \mathbb{R}^2 : \, y = ax + b\}.$$

Denote by $I(P,L)$ the number of incidences between lines in L and points in P:

$$I(P,L) = |\{(p,\ell) \in P \times L \text{ such that } p \in \ell\}|.$$

Trivially, we have that $|I(P,L)| \leq |P||L|$. Nevertheless, one can obtain a better bound by simply exploiting Cauchy-Scwartz inequality.

Proposition 4.1. *Let P be a set of points and L a set of lines in $\mathbb{R}^2$. Then*

$$I(P,L) \leq \min\left\{|P|^{1/2}|L| + |P|, |L|^{1/2}|P| + |L|\right\}.$$

Proof. In first place, for a point p and a line ℓ we define the indicator function

$$\mathbb{I}_\ell(p) = \begin{cases} 1 & \text{if } p \in \ell, \\ 0 & \text{otherwise.} \end{cases}$$

Then it follows from Cauchy-Schwartz inequality

$$I(P,L)^2 = \big(\sum_{\ell\in L}\sum_{p\in P}\mathbb{I}_\ell(p)\big)^2 \le |L|\sum_{\ell\in L}\big(\sum_{p\in P}\mathbb{I}_\ell(p)\big)^2 = |L|\sum_{\ell\in L}\sum_{p_1,p_2\in P}\mathbb{I}_\ell(p_1)\mathbb{I}_\ell(p_2).$$

Note that if $p_1 = p_2$ the contribution to the previous sum is precisely $I(P,L)$ and as long as $p_1 \neq p_2$ then there exist at most one line with $\mathbb{I}_\ell(p_1)\mathbb{I}_\ell(p_2) = 1$, from where we derive

$$\sum_{\ell\in L}\sum_{p_1,p_2\in P}\mathbb{I}_\ell(p_1)I_\ell(p_2) \le I(P,L) + |P|^2.$$

Thus

$$I(P,L)^2 - |L|\cdot I(P,L) - |L||P|^2 \le 0,$$

or equivalently

$$I(P,L) \le \frac{|L| + \sqrt{|L|^2 + 4|L||P|^2}}{2} \le |L|^{1/2}|P| + |L|.$$

For the dual inequality, note that

$$I(P,L)^2 = \big(\sum_{p\in P}\sum_{\ell\in L}\mathbb{I}_\ell(p)\big)^2 \le |P|\sum_{p\in P}\big(\sum_{\ell\in L}\mathbb{I}_\ell(p)\big)^2 = |P|\sum_{p\in P}\sum_{\ell_1,\ell_2\in L}\mathbb{I}_{\ell_1}(p)\mathbb{I}_{\ell_2}(p).$$

Once again, the contribution from $\ell_1 = \ell_2$ is precisely $I(P,L)$ and when $\ell_1 \neq \ell_2$ clearly $\mathbb{I}_{\ell_1}(p)\mathbb{I}_{\ell_2}(p) = 1$ for at most one pont p, from which

$$I(P,L)^2 - |P|\cdot I(P,L) - |P||L|^2 \le 0.$$

Once again, it implies that

$$I(P,L) \le \frac{|P| + \sqrt{|P|^2 + 4|P||L|^2}}{2} \le |P|^{1/2}|L| + |P|.$$

□

Remark 6. *The previous argument is not only valid for $\mathbb{R}$ but the same bounds hold for any field (in particular for finite fields). Since we only exploited two basic geometric facts: two points determine a unique line and two lines intersect in at most one point.*

In 1983 Szemerédi and Trotter [7] proved a tight bound for the quantity $I(P,L)$ in $\mathbb{R}$. Their result is known as the Szemerédi-Trotter Theorem.

Theorem 4.2 (Szemeredi-Trotter [7])**.** *Let P be a set of points and L a set of lines in $\mathbb{R}^2$. Then the number of incidences satisfies*

$$I(P,L) \le 4|L|^{2/3}|P|^{2/3}|L| + 4|P| + |L|.$$

We will now show the elegant argument from Elekes, who exploited the previous result to prove a bound for the sum-product problem.

Theorem 4.3 (Elekes [3])**.** *Let $A \subset \mathbb{R}$ be a finite subset. Then: $|A+A|^2|A\cdot A|^2 \gg |A|^5$, and in particular*

$$\max\{|A+A|, |A\cdot A|\} \gg |A|^{4/5}.$$

Proof. Define the set of points $P = (A+A)\times(A\cdot A) \subset \mathbb{R}^2$ and the set of lines $L = \{y = a(x-b) : a,b \in A\}$, and note that $|P| = |A+A||A\cdot A|$ and $|L| = |A|^2$.

On one hand, observe that for every line $y = a(x-b)$ there exists at least $|A|$ points in P: for every $c \in A$ the points $(x,y) = (b+c, ac) \in P$ belong to such line. Thus

$$I(P,L) \ge |A||L| = |A|^3. \tag{2}$$

On the other hand, it follows from Szemerédi-Trotter that

$$I(P,L) \ll |L|^{2/3}|P|^{2/3}|L| + |P| + |L| = |A|^{4/3}|A+A|^{2/3}|A\cdot A|^{2/3} + |A+A||A\cdot A| + |A|^2,$$

which combined with (2) implies the desired bound. □

4.2 The analogue in finite fields

Let us note that in $\mathbb{F}_q$ we cannot expect to obtain the same bounds as in Theorem 4.2. In particular, the bounds in Proposition 4.1 are tight in $\mathbb{F}_q$: if we take $P = \mathbb{F}_q^2$ and a set of q lines in L, it is clear that every line contributes with exactly q coincidences

$$I(P, L) = q^2 = |P|^{1/2}|L|.$$

In first place, Bourgain, Katz and Tao exploited Theorem 2.4 in [1] to obtain an incidence theorem between the number of incidences of points and lines in prime fields.

Theorem 4.4 (Bourgain-Katz-Tao). *For every $\epsilon > 0$, there exists a positive δ such that if $N = \max\{|P|, |L|\} \leq p^{2-\epsilon}$, then*

$$I(P, L) \ll N^{3/2-\delta}.$$

Observe that this bound improves the bound from Proposition 4.1 in this range, which gives us $I(P, L) \ll N^{3/2}$.

On the other side, Vinh [8] proved an incidence theorem in finite fields to exploit Elekes method and derive Theorem 2.6. In particular, he showed the following result.

Theorem 4.5 (Vinh). *Let $P \subset \mathbb{F}_q^2$ a set of points and L a set of lines, then*

$$I(P, L) \leq \frac{|P||L|}{q} + \sqrt{q|P||L|}.$$

Proof of Theorem 2.6 from Theorem 4.5 As we did in Elekes proof, consider the set of points $P = (A + A) \times (A \cdot A) \subset \mathbb{F}_q^2$ and the set of lines $L = \{y = a(x - b) : a, b \in A\}$, and note that $|P| = |A + A||A \cdot A|$ and $|L| = |A|^2$.

On one hand, observe that for every line $y = a(x - b)$ there exists at least $|A|$ points in P: for every $c \in A$ the points $(x, y) = (b + c, ac) \in P$ belong to such line. Thus

$$I(P, L) \geq |A||L| = |A|^3. \tag{3}$$

On the other hand, it follows from Theorem 4.5 that

$$I(P, L) \leq \frac{|P||L|}{q} + \sqrt{q|P||L|} = \frac{|A + A||A \cdot A||A|^2}{q} + \sqrt{q|A + A||A \cdot A||A|^2},$$

which combined with (3) gives us

$$|A|^2 \leq \frac{|A + A||A \cdot A||A|}{q} + \sqrt{q|A + A||A \cdot A|}. \tag{4}$$

If $|A + A||A \cdot A| < q^3|A|^{-2}$, then from (4) it follows that

$$|A|^2 \ll \sqrt{q|A + A||A \cdot A|}$$

which implies that $\max\{|A + A|, |A \cdot A|\} \gg \frac{|A|^2}{\sqrt{q}}$.

It $|A + A||A \cdot A| \geq q^3|A|^{-2}$, it follows from (4) that

$$|A|^2 \ll \frac{|A + A||A \cdot A||A|}{q}$$

which implies that $\max\{|A + A|, |A \cdot A|\} \gg \sqrt{|A|q}$. Combining this two bounds we obtained the desired result. □

These same ideas have been used in different variations of the sum-product problem.

References

[1] J. Bourgain, N. Katz and T. Tao, 'A sum-product estimate in finite fields, and applications' *Geom. Funct. Anal.* **14** (2004), no. 1, 27–57.

[2] T. Cochrane and C. Pinner, 'Sum-product estimates applied to Waring's problem *modp*', *Integers* **8** (2008).

[3] F. Elekes, 'On the number of sums and products', *Acta Arith.* **81** (1997), 365–367.

[4] P. Erdős, 'Some remarks on number theory' *Riveon Lematematika* **9** (1955), 45–48.

[5] K. Ford, 'The distribution of integers with a divisor in a given interval', *Annals of Math.*, **168** (2008), 367–433.

[6] M. Garaev, 'An explicit sum–product estimate in $\mathbb{F}_p$', *Int. Math. Res. Not.* (11) (2007).

[7] E. Szemerédi and W. T. Trotter, Jr., 'Extremal problems in discrete geometry', *Combinatorica* **3** (1983), 381–392.

[8] L-A. Vinh, 'The Szemerédi-Trotter type theorem and the sum-product estimate in finite fields', *European J. Combin.* **32** (8) (2011), 1177–1181.

[9] A. Winterhof, 'On Waring's problem in finite fields', *Acta Arith.* **87** (2) (1998), 171–177.