SZEMERÉDI-TROTTER TYPE RESULTS IN ARBITRARY FINITE FIELDS

Ali Mohammadi
School of Mathematics, Institute for Research in Fundamental Sciences (IPM), Tehran, Iran
A.Mohammadi@ipm.ir

Received: 4/28/19, Accepted: 1/7/20, Published: 1/22/20

Abstract

Let q be a power of a prime and $\mathbb{F}_q$ the finite field consisting of q elements. We prove explicit upper bounds on the number of incidences between lines and Cartesian products in $\mathbb{F}_q^2$. We also use our results on point-line incidences to give new sum-product type estimates concerning sums of reciprocals.

1. Introduction

Let F be an arbitrary field. Given a finite set of points P and a finite set of lines L in the plane F^2, we define the number of incidences between P and L by

$$I(P,L) = |\{(p,l) \in P \times L : p \in l\}|.$$

An elementary argument, which involves an application of the Cauchy-Schwarz inequality, yields the trivial bound

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

See [7, Corollary 5.2] for a proof of the above inequality. In particular, in the critical case $|P| = |L| = N$, we have $I(P,L) \leq N^{3/2}$.

In the case $F = \mathbb{R}$, Szemerédi and Trotter [26] proved the bound

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

A construction due to Elekes [9] demonstrates that this bound is sharp up to constants.

Let p be a prime, $\mathbb{F}_q$ the finite field consisting of $q = p^m$ elements and $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. The primary purpose of this paper is to establish nontrivial upper bounds on $I(P,L)$ for sets of points P and lines L in $\mathbb{F}_q^2$. An immediate obstacle in this

setting is the presence of nontrivial subfields. Given a subfield G of $\mathbb{F}_q$, let $P = G \times G$ and let $L = \{l_{a,b} : a, b \in G\}$, where $l_{a,b} = \{(x, y) \in \mathbb{F}_q^2 : y = ax + b\}$. Then $|P| = |G|^2$, $|L| \approx |G|^2$ and $I(P, L) \approx |G|^3$. Therefore, in this example, the bound (1) is optimal up to constants. We deduce that such point sets, as well as their image under any affine transformations, must be avoided in order to ensure a nontrivial incidence bound holds.

Let $X(P) = \{x : (x, y) \in P\}$. Jones [12] proved that, given a set of points P and lines L in $\mathbb{F}_q^2$ with $|P| = |L| = N$, there exists an absolute constant $\gamma > 0$ such that the bound

$$I(P, L) \ll N^{3/2-1/12838} \tag{2}$$

holds if P satisfies the following two conditions.

(i) For all subfields G and elements c, d in $\mathbb{F}_q$,

$$|X(P) \cap (cG + d)| \leq \max\{|G|^{1/2}, \gamma N^{2560/6419}\}.$$

(ii) For every subfield G in $\mathbb{F}_q$ with $|G| \geq \gamma N^{2560/6419}$, $X(P)$ intersects strictly fewer than $\max\{|G|^{1/2}, \gamma N^{2560/6419}\}/2$ distinct translates $G + d$ of G.

One expects that the first of the two restrictions above should be sufficient for a nontrivial bound on $I(P, L)$ to hold and it should be clear that, largely due to the additional restriction, this result is not well-suited for most applications. In this paper, with some applications in mind, we focus only on the case where P is a Cartesian product and prove stronger incidence bounds which hold under weaker restrictions.

For large sets of points and lines, with $|P|, |L| \geq q$, Vinh [28] proved the bound

$$\left| I(P, L) - \frac{|P||L|}{q} \right| \leq (q|P||L|)^{1/2}. \tag{3}$$

Also see [18] for an elementary proof of this result.

In the regime of small sets, Stevens and de Zeeuw [25] proved the following result. Let $A, B \subset F$, with $|B| \leq |A|$ and let L be a set of lines in F^2 such that $|L|^3 \geq |A|^2|B|$. If F has positive characteristic p, assume $|B||L| \ll p^2$. Then

$$I(A \times B, L) \ll |A|^{1/2}|B|^{3/4}|L|^{3/4} + |L|.$$

As outlined in [25, Example 5], this bound is optimal for certain sets of points and lines. However, in the setting $F = \mathbb{F}_q$, if q is a large power of p then the above estimate becomes restricted to very small sets of points and lines. The main ingredient in the proof of the above result is a bound on the number of incidences between points and planes due to Rudnev [21]. Indeed, [21] has been the driving force behind much of the recent progress on sum-product type problems as well as

certain related geometric questions in fields of positive characteristic. A survey on some of such developments is provided in [22]. However, we note that these new techniques appear to be ineffective in dealing with general subsets of $\mathbb{F}_q$.

Prior to the appearance of Rudnev's result on point-plane incidences, sum-product estimates provided the key tool in the study of point-line incidences in finite fields. For sets $A, B \subset \mathbb{F}_q$ we define the sum set $A+B = \{a+b : a \in A, b \in B\}$ and similarly define the difference set $A-B$, the product set AB and the ratio set A/B. To avoid dividing by zero, it is assumed throughout the paper that all sets contain strictly more than one element and exclude zero.

Bourgain, Katz and Tao [7] proved the first qualitative sum-product estimate in $\mathbb{F}_p$, which states that for any $\alpha > 0$ there exists a $\beta = \beta(\alpha) > 0$ such that if $A \subset \mathbb{F}_p$ and $p^\alpha < |A| < p^{1-\alpha}$, then

$$\max\{|A+A|, |AA|\} \gg_\alpha |A|^{1+\beta}.$$

As a corollary, they proved that, for any $0 < \epsilon < 2$ there exists a $\delta = \delta(\epsilon) > 0$ such that, given a set of points P and a set of lines L in $\mathbb{F}_p^2$, if $|P|, |L| \leq N = p^\epsilon$ then

$$I(P, L) \ll N^{3/2-\delta}. \tag{4}$$

This result is based, roughly, on the observation that if there are too many incidences between elements of P and L, then one can identify a set $A \subset \mathbb{F}_p$, of cardinality close to $|P|^{1/2}$, such that $|A+A|$ and $|AA|$ are both small. Consequently, through the use of a sum-product estimate, one concludes that A must occupy nearly all of $\mathbb{F}_p$.

In a similar vein, building on the subsequent progress on the sum-product problem, Helfgott and Rudnev [11] and later Jones [13] obtained explicit variants of the above incidence result.

In this paper, we use sum-product estimates, as well as related techniques, to establish nontrivial upper bounds on the number of collinear triples $T(A, B)$ formed by a Cartesian product $A \times B$, where $A, B \subset \mathbb{F}_q$. Then, in the same manner as [1, Corollary 6], we use the acquired estimates of $T(A, B)$ to bound $I(A \times B, L)$ given any set of lines L in $\mathbb{F}_q^2$. Formally, we define $T(A, B)$ as the number of sextuples $(a_1, a_2, a_3, b_1, b_2, b_3) \in A^3 \times B^3$ satisfying

$$(a_2 - a_1)(b_3 - b_1) = (a_3 - a_1)(b_2 - b_1). \tag{5}$$

For the sake of simplicity, we write $T(A)$ instead of $T(A, A)$. We observe the trivial upper bound

$$T(A, B) \leq |A|^2|B|^2 \cdot \min\{|A|, |B|\}. \tag{6}$$

Clearly, for all $c_1, c_2 \in \mathbb{F}_q^*$ and all $d_1, d_2 \in \mathbb{F}_q$, we have

$$T(c_1A + d_1, c_2B + d_2) = T(A, B).$$

Additionally, note that (6) becomes an equality if $A = B = G$ for some subfield $G \subset \mathbb{F}_q$. However, one expects that a nontrivial upper bound on $T(A, B)$ holds as long as either A or B does not correlate with any sets of the form $cG + d$, for subfields G and elements $c, d \in \mathbb{F}_q$.

Let $T^*(A, B)$ denote the number of nontrivial collinear triples of $A \times B$, defined as the number of sextuples $(a_1, a_2, a_3, b_1, b_2, b_3) \in A^3 \times B^3$ satisfying

$$(a_2 - a_1)(b_3 - b_1) = (a_3 - a_1)(b_2 - b_1) \neq 0. \tag{7}$$

Then, assuming $|B| \leq |A|$, it follows that

$$T(A, B) \approx T^*(A, B) + |A|^3|B|. \tag{8}$$

The term $|A|^3|B|$ can be interpreted as the contribution to the number of collinear triples coming from $|B|$ horizontal lines. It is worth noting that if $|B| \ll |A|^{1/2}$ then (6) and (8) together imply $T(A, B) \approx |A|^3|B|$.

We mention that for $A \subset \mathbb{F}_q$ with $|A| \ll p^{2/3}$, Aksoy Yazici et al. [1] proved the bound $T(A) \ll |A|^{9/2}$. Furthermore, $T(A)$ has been studied extensively by Murphy et al. [19] in the context of prime fields.

Define $L(P)$ to be the number of distinct lines determined by pairs of points of $P \subset \mathbb{F}_q^2$. As a further application of our bounds on $T(A, B)$, we prove nontrivial lower bounds on $L(P)$ for Cartesian products $P = A \times B$, with $A, B \subset \mathbb{F}_q$. See [1, 25] for stronger estimates which hold for sets that are bounded in size in terms of the characteristic p.

Finally, we obtain an explicit lower bound on the quantity $\max\{|A + A|, |1/A + 1/A|\}$ for sets $A \subset \mathbb{F}_q$ which are not close in size to any proper subfields. This result was used recently by Macourt and Shparlinski [17] to bound certain double sums of Kloosterman sums. Also see [2] for other closely related potential applications.

Asymptotic Notation

For positive real numbers X and Y, we write $X \ll Y$, $Y \gg X$, $X = O(Y)$ and $Y = \Omega(X)$ to all mean that $X \leq cY$ for some absolute constant $c > 0$. If the constant c depends on a parameter ϵ, we write $X = O_\epsilon(Y)$ etc. If $X \ll Y$ and $Y \ll X$, we write $X = \Theta(Y)$ or $X \approx Y$.

2. Main Results

2.1. Incidence Bounds

Our first result is based on some techniques introduced in [11], which also underlie the incidence result of Jones [12]. However, our approach differs from [12] in that

we consider only Cartesian products, thereby relaxing the required constraints on the point sets.

Theorem 1. *Let $A, B \subset \mathbb{F}_q$ with $|B| \le |A|$ and let L be a set of lines in $\mathbb{F}_q^2$. Suppose that*

$$|A \cap (cG + d)| \ll \max\left\{|G|^{1/2}, |A|^{31/191}|B|^{129/191}\right\}$$

for all proper subfields G of $\mathbb{F}_q$ and all elements $c, d \in \mathbb{F}_q$. Then

$$T(A,B) \ll |A|^{383/191}|B|^{571/191} + q^{-1/103}|A|^{207/103}|B|^3 + |A|^3|B|, \tag{9}$$

$$I(A \times B, L) \ll \left(|A|^{383/573}|B|^{571/573} + q^{-1/309}|A|^{207/309}|B| + |A||B|^{1/3}\right)|L|^{2/3} + |L|, \tag{10}$$

$$L(A \times B) \gg \min\left\{|A|^{380/191}|B|^{4/191}, q^{2/103}|A|^{204/103}, |B|^4\right\}. \tag{11}$$

In the case $B = A$, we obtain the following improvement of Theorem 1.

Theorem 2. *Let $A \subset \mathbb{F}_q$ and let L be a set of lines in $\mathbb{F}_q^2$. Suppose that*

$$|A \cap (cG + d)| \ll \max\left\{|G|^{1/2}, |A|^{51/52}\right\}, \tag{12}$$

for all proper subfields G of $\mathbb{F}_q$ and all elements $c, d \in \mathbb{F}_q$. Then, we have the estimates

$$T(A) \ll |A|^{5-1/104} + q^{-1/95}|A|^{5+1/95}, \tag{13}$$

$$I(A \times A, L) \ll \left(|A|^{173/104} + q^{-1/285}|A|^{476/285}\right)|L|^{2/3} + |L|, \tag{14}$$

$$L(A \times A) \gg \min\{|A|^{2+1/52}, q^{2/95}|A|^{2-2/95}\}. \tag{15}$$

To compare the above result with (2), let $P = A \times A$ for a set $A \subset \mathbb{F}_q$, which satisfies restriction (12). Then given any set of lines L in $\mathbb{F}_q^2$, if $|L| = |P| = N$, by (14) we have

$$I(P, L) \ll N^{3/2-1/624} + q^{-1/285}N^{3/2+1/570}.$$

This also improves on (3) in the range $N < q^{1+1/311}$. Given any sets $A, B \subset \mathbb{F}_q$, with $|B| \le |A|$, by the Cauchy-Schwarz inequality we have

$$T(A,B) \ll T(A)^{1/2}T(B)^{1/2} + |A|^3|B|. \tag{16}$$

Suppose that the sets A and B both satisfy condition (12) and $|A| \ll q^{1/2}$. Then by Theorem 2, together with inequality (16), we obtain

$$T(A,B) \ll |A|^{519/208}|B|^{519/208} + |A|^3|B|. \tag{17}$$

It follows that estimate (9) is stronger than (17) in the range

$$|A|^{1/2} < |B| \ll |A|^{1-c},$$

where $c = 174/19639 < 1/112$.

Our next result can be used to obtain nontrivial upper bounds on $T(A)$, for sets $A \subset \mathbb{F}_q$, if either $|A + A|$ or $|A - A|$ is small.

Theorem 3. *Let $A \subset \mathbb{F}_q$. Suppose that there exists some $\delta > 0$ such that*

$$|A \cap (cG + d)| \ll \max\{|G|^{1/2}, |A|^{1-\delta}\} \tag{18}$$

for all proper subfields G of $\mathbb{F}_q$ and all elements $c, d \in \mathbb{F}_q$. Then

$$T(A) \ll \log|A| \cdot \big(|A+A|^{7/4}|A|^3 + |A+A|^{6/5}|A|^{18/5} + |A|^{5-\delta/2} + |A+A|^{7/4}|A|^{7/2}q^{-1/4}\big). \tag{19}$$

The same estimate holds with the sum set $A+A$ replaced by the difference set $A-A$.

In particular, assuming $|A+A| \approx |A|$, we obtain significant improvements over the estimates of Theorem 2.

Corollary 1. *Let $A \subset \mathbb{F}_q$. Suppose that $|A+A| \approx |A|$ and*

$$|A \cap (cG + d)| \ll \max\{|G|^{1/2}, |A|^{3/5}\} \tag{20}$$

for all elements $c, d \in \mathbb{F}_q$ and proper subfields G. Then, for any set of lines L in $\mathbb{F}_q^2$, we have the estimates

$$T(A) \ll \log|A| \cdot (|A|^{5-1/5} + q^{-1/4}|A|^{5+1/4}), \tag{21}$$

$$I(A \times A, L) \ll \log|A|^{1/3} \cdot (|A|^{24/15} + q^{-1/12}|A|^{21/12})|L|^{2/3} + |L|, \tag{22}$$

$$L(A \times A) \gg \log|A|^{-2} \cdot \min\{|A|^{2+2/5}, q^{1/2}|A|^{2-1/2}\}. \tag{23}$$

2.2. Applications

Based on Theorem 2, we obtain the following result which provides an explicit variant of [2, Theorem 4] for subsets of $\mathbb{F}_q$. Also see [5] for sharp bounds on sums of reciprocals of intervals in $\mathbb{F}_p$.

Corollary 2. *Let $A, B \subset \mathbb{F}_q$. Suppose that*

$$|(A+B)^{-1} \cap (cG + d)| \ll \max\{|G|^{1/2}, |A+B|^{51/52}\} \tag{24}$$

for all proper subfields G and elements c, d in $\mathbb{F}_q$. Then

$$E_+(1/A, 1/B) \ll \Big(|A+B|^{173/104} + q^{-1/285}|A+B|^{476/285}\Big)|B|^{4/3}. \tag{25}$$

Consequently, if condition (24) *holds with $B = A$, then*

$$\max\{|A+A|, |1/A+1/A|\} \gg \min\{|A|^{1+1/831}, q^{1/761}|A|^{1-1/761}\}. \tag{26}$$

If condition (24) *holds with $B = A^{-1}$, then*

$$|A+1/A| \gg \min\{|A|^{1+1/831}, q^{1/761}|A|^{1-1/761}\}. \tag{27}$$

Alternatively, estimates (26) *and* (27) *hold if the cardinality of A does not lie in the intervals $(|G|^{1/2-1/1664}, |G|^{1+1/51})$ for all proper subfields G of $\mathbb{F}_q$.*

For a set $A \subset \mathbb{F}_q$, with a small sum set, we use Corollary 2 to obtain a nontrivial upper bound on the number of solutions to the hyperbola $xy = \alpha$, where $(x, y) \in A \times A$. See [1, Corollary 15] for a stronger analogue of this result which holds if $|A| < p^{5/8}$. Also see [8] for sharp estimates concerning intervals in $\mathbb{F}_p$.

Corollary 3. *Let $A \subset \mathbb{F}_q$. Suppose that*

$$|(A+A)^{-1} \cap (cG+d)| \ll \max\{|G|^{1/2}, |A+A|^{47/48}\} \tag{28}$$

for all proper subfields G and elements c, d in $\mathbb{F}_q$. Then, for any $\alpha \in \mathbb{F}_q^*$, we have

$$|A \cap \alpha/A| \ll |A+A|^{1-1/832} + q^{-1/760}|A+A|^{1+1/760}. \tag{29}$$

Alternatively, estimate (29) *holds if $|A| \notin (|G|^{1/2-1/1664}, |G|^{1+1/47})$ for all proper subfields $G \subset \mathbb{F}_q$.*

We use Theorem 3 to obtain the following improvement of estimate (26) for additive groups.

Corollary 4. *Let $A \subset \mathbb{F}_q$ be an additive group. Suppose that*

$$|A^{-1} \cap (cG+d)| \ll \max\{|G|^{1/2}, |A|^{5/7}\} \tag{30}$$

for all proper subfields G and elements c, d in $\mathbb{F}_q$. Then

$$|1/A \pm 1/A| \gg (\log|A|)^{-1/3} \cdot \min\{|A|^{1+1/21}, q^{1/19}|A|^{1-1/19}\}. \tag{31}$$

Alternatively, estimate (31) *holds if $|A| \notin (|G|^{1/2}, |G|^{1+2/5})$ for all proper subfields $G \subset \mathbb{F}_q$.*

3. Preliminaries

We require an extension of a sum-product type estimate due to Roche-Newton [20]. Since [20] has not been peer-reviewed, we provide a full proof of this result in Appendix 4.2, which closely follows the original arguments.

Lemma 1. *Let $A \subseteq \mathbb{F}_q$ and let $0 < \eta < 1/8$. Suppose $|A| \ll q^{1/2}$ and that*

$$|A \cap cG| \leq \max\left\{C|G|^{1/2}, \eta|A|\right\} \tag{32}$$

for all proper subfields G of $\mathbb{F}_q$, elements $c \in \mathbb{F}_q$ and some constant $C > 0$. Then either

$$|A \pm A|^7 |A/A|^4 \gg_\eta |A|^{12} \qquad \text{or} \qquad |A \pm A|^6 |A/A|^5 \gg_\eta |A|^{12}.$$

If $|A| > \eta^{-1} q^{1/2}$, irrespective of condition (32)*, we have*

$$|A \pm A|^7 |A/A|^4 \gg_\eta |A|^{10} q.$$

Remark 1. Following a similar approach as [10, Theorem 1] or [28, Corollary 2], for any set $A \subset \mathbb{F}_q$, one can establish the bound

$$\max\{|A \pm A|, |A/A|\} \gg \min\{|A|^{1/2}q^{1/2}, |A|^2/q^{1/2}\}.$$

This bound is nontrivial if $|A| > q^{1/2}$ and, as demonstrated in [10], it is optimal up to constants if $|A| > q^{2/3}$. We point out that Lemma 1 improves on this bound if $|A| < q^{13/24}$.

Given sets $A, B \subseteq \mathbb{F}_q$, we define the multiplicative energy between A and B by

$$E_\times(A, B) = |\{(a_1, a_2, b_1, b_2) \in A^2 \times B^2 : a_1b_1 = a_2b_2\}|. \tag{33}$$

We write simply $E_\times(A)$ instead of $E_\times(A, A)$. Using the Cauchy-Schwarz inequality, we get

$$E_\times(A, B) \leq E_\times(A)^{1/2}E_\times(B)^{1/2}. \tag{34}$$

See [27, Corollary 2.10] for a proof of the above inequality.

One may recover a bound on the multiplicative energy of subsets of $\mathbb{F}_q$ from the proof of [16, Theorem 1.4]. We state a slightly generalized version of this bound below and give a sketch of the proof in Appendix 4.2.

Lemma 2. *Let $A \subseteq \mathbb{F}_q$. Suppose that*

$$|A \cap cG| \ll \max\left\{|G|^{1/2}, |A|^{1-\delta}\right\} \tag{35}$$

for all proper subfields G of $\mathbb{F}_q$, elements $c \in \mathbb{F}_q$ and some fixed $\delta > 0$. Then

$$E_\times(A) \ll \log|A| \cdot \big(|A + A|^{7/4}|A| + |A + A|^{6/5}|A|^{8/5} + |A|^{3-\delta/2} + |A + A|^{7/4}|A|^{3/2}q^{-1/4}\big). \tag{36}$$

In the above estimate, one can replace the sum set $A+A$ by the difference set $A-A$.

For $X \subset \mathbb{F}_q$, we define the quotient set of X by

$$R(X) = \left\{\frac{x_1 - x_2}{x_3 - x_4} : x_1, x_2, x_3, x_4 \in X, x_3 \neq x_4\right\}.$$

We make frequent use of the following basic variant of [27, Lemma 2.50].

Lemma 3. *Let $X \subset \mathbb{F}_q$ and $r \in \mathbb{F}_q$. If $r \notin R(X)$, then for any nonempty subsets $X_1, X_2 \subseteq X$, we have $|X_1||X_2| = |X_1 + rX_2|$.*

Proof. If two distinct pairs $(x_1, x_2), (y_1, y_2) \in X_1 \times X_2$ satisfy $x_1 + rx_2 = y_1 + ry_2$, it follows that $r = (x_1 - y_1)/(y_2 - x_2) \in R(X)$. Hence if $r \notin R(X)$, then the map $(x_1, x_2) \mapsto x_1 + rx_2$ is injective on $X_1 \times X_2$, which implies the required result. □

We state a corollary of Lemma 3, which also appears in [27, Corollary 2.51].

Lemma 4. *Let $X \subset \mathbb{F}_q$ with $|X| > q^{1/2}$, then $R(X) = \mathbb{F}_q$.*

The next lemma has been extracted from the proof of the main result in [16]. It serves as a stronger substitute for a similar result by Katz and Shen [15]. A precise statement of the latter can also be found in [12, Lemma 6].

Lemma 5. *Let $X \subset \mathbb{F}_q$. Suppose that*

$$1 + R(X) \subseteq R(X) \quad \text{and} \quad X \cdot R(X) \subseteq R(X).$$

Then $R(X) = \mathbb{F}_X$, where $\mathbb{F}_X$ denotes the subfield of $\mathbb{F}_q$ generated by X.

The following lemma combines [6, Lemma 3] and [16, Lemma 2.4].

Lemma 6. *Let $X \subset \mathbb{F}_q$ and let $X^{'}$ be any subset of X with $|X^{'}| \approx |X|$. If $|R(X)| \gg |X|^2$, then there exists $r \in R(X)$, such that $|X^{'} + rX^{'}| \gg |X|^2$. If $|X| > q^{1/2}$, then there exists $r \in \mathbb{F}_q^*$ such that $|X^{'} + rX^{'}| \gg q$.*

Next, we recall a covering lemma, which can be found in [23].

Lemma 7. *Let $X, Y \subseteq \mathbb{F}_q$. Then, for any $0 < \epsilon < 1$, there exists a constant $C(\epsilon)$, such that at least $(1-\epsilon)|X|$ elements of X can be covered by*

$$C(\epsilon) \cdot \min\left\{\frac{|X+Y|}{|Y|}, \frac{|X-Y|}{|Y|}\right\}$$

translates of Y.

The following two lemmas provide well-known variants of the Plünnecke-Ruzsa inequality. Both lemmas also appear in [14].

Lemma 8. *Let $X, Y_1, \ldots, Y_k \subset \mathbb{F}_q$. Then*

$$|Y_1 + \cdots + Y_k| \leq \frac{|X+Y_1| \cdots |X+Y_k|}{|X|^{k-1}}.$$

Lemma 9. *Let $X, Y_1, \ldots, Y_k \subset \mathbb{F}_q$. For any $0 < \epsilon < 1$, there exists a subset $X^{'} \subseteq X$, with $|X^{'}| \geq (1-\epsilon)|X|$ such that*

$$|X^{'} + Y_1 + \cdots + Y_k| \ll_{\epsilon,k} \frac{|X+Y_1| \cdots |X+Y_k|}{|X|^{k-1}}.$$

For any nonempty sets X, Y in an abelian group and any set $G \subseteq X \times Y$, we define the partial difference set of X and Y as

$$X \overset{G}{-} Y = \{x - y : (x, y) \in G\}.$$

This notation is extended to other operations in a similar way. We recall two different formulations of the Balog-Szemerédi-Gowers theorem. Lemma 10 below is due to Bourgain and Garaev [4].

Lemma 10. *Let X, Y be subsets of an abelian group and $G \subseteq X \times Y$. Then, there exists $X^{'} \subseteq X$ with $|X^{'}| \gg |G|/|Y|$ such that*

$$|X^{'} - X^{'}| \ll \frac{|X \overset{G}{-} Y|^4 |X|^4 |Y|^3}{|G|^5}.$$

See [27, Theorem 2.29] for a proof of the following formulation.

Lemma 11. *Let X, Y be subsets of an abelian group and $G \subseteq X \times Y$. Then, there exist subsets $X^{'} \subseteq X$ and $Y^{'} \subseteq Y$ with*

$$|X^{'}| \gg \frac{|G|}{|Y|} \quad \text{and} \quad |Y^{'}| \gg \frac{|G|}{|X|}$$

such that

$$|X^{'} + Y^{'}| \ll \frac{|X \overset{G}{+} Y|^3 |X|^4 |Y|^4}{|G|^5}.$$

The following lemma is due to Bourgain [3]. A proof is also provided in [12, Lemma 8].

Lemma 12. *Let $X, Y \subset \mathbb{F}_q$ and let $M = \max_{y \in Y} |X + yX|$. Then there exist elements $x_1, x_2, x_3 \in X$ such that*

$$|(X - x_1) \cap (x_2 - x_3)Y| \gg \frac{|Y||X|}{M}.$$

We use the following pigeonholing argument on numerous occasions throughout the paper. See [12, Lemma 9] for a proof.

Lemma 13. *Let X be a finite set and let f be a function such that $f(x) > 0$ for all $x \in X$. Suppose that*

$$\sum_{x \in X} f(x) \geq K.$$

Let $Y = \{x \in X : f(x) \geq K/2|X|\}$. Then

$$\sum_{y \in Y} f(y) \geq \frac{K}{2}.$$

Furthermore, if $f(x) \leq M$ for all $x \in X$, then $|Y| \geq K/(2M)$.

Throughout Lemma 14 below, with a slight abuse of notation, we use $T(P)$ to denote the number of collinear triples formed by a set of points $P \subset \mathbb{F}_q^2$. Also recall that $L(P)$ denotes the number of distinct lines determined by pairs of points in P.

Lemma 14. *Let P be a set of points and L a set of lines in $\mathbb{F}_q^2$. For $k \geq 1$, define*

$$I_k(P,L) = |\{(p_1,\dots,p_k,l) \in P^k \times L : p_1,\dots,p_k \in l\}|.$$

Then, we have the inequalities

$$I(P,L) \leq I_k(P,L)^{1/k}|L|^{(k-1)/k}, \tag{37}$$

$$I(P,L) \ll T(P)^{1/3}|L|^{2/3} + |L|, \tag{38}$$

$$|P|^2 \ll |L(P)|^{1/3}T(P)^{2/3}. \tag{39}$$

Proof. For a line $l \in L$, we use 1_l to denote the indicator function of l. Namely, given a point $p \in \mathbb{F}_q^2$, we have $1_l(p) = 1$ if $p \in l$ and 0 otherwise. Then, clearly

$$I(P,L) = \sum_{l\in L}\sum_{p\in P} 1_l(p).$$

For $k \geq 1$, we obtain inequality (37) by an application of Hölder's inequality and the observation that

$$I_k(P,L) = \sum_{l\in L}\Big(\sum_{p\in P} 1_l(p)\Big)^k. \tag{40}$$

Next, we claim that $I_3(P,L) \ll I_3(P,L(P)) + |L|$. To see this, note that the contribution to $I_3(P,L)$ coming from lines containing exactly one point is bounded by $|L|$ and the contribution from lines containing two or more points of P is of order $I_3(P,L(P))$. Then (38) follows from (37), with $k = 3$, and the simple observation that $I_3(P,L(P)) = T(P)$.

To prove (39), note that by Hölder's inequality, we have

$$\sum_{l\in L(P)}\Big(\sum_{p\in P} 1_l(p)\Big)^2 \leq \Big(\sum_{l\in L(P)}\Big(\sum_{p\in P} 1_l(p)\Big)^3\Big)^{2/3}\Big(\sum_{l\in L(P)} 1\Big)^{1/3}.$$

Recalling identity (40), this reduces to

$$I_2(P,L(P)) \leq I_3(P,L(P))^{2/3}L(P)^{1/3}.$$

Then, since $I_3(P,L(P)) = T(P)$ and $I_2(P,L(P)) \gg |P|^2$, the required inequality follows. □

For sets $A, B \subset \mathbb{F}_q$, we define the additive energy $E_+(A,B)$, $E_+(A)$ as the additive analogue of (33). We have the following consequence of the Cauchy-Schwarz inequality

$$E_+(A,B)|A \pm B| \geq |A|^2|B|^2. \tag{41}$$

The following lemma is a slight variation of a result due to Bourgain [2, Theorem 4.1]. It can also be found in [24, Lemma 14].

Lemma 15. *Let $A, B \subset \mathbb{F}_q$. Then*

$$E_+(1/A, 1/B) \le I(P, L), \tag{42}$$

where $P = (A+B)^{-1} \times (A+B)^{-1}$ and L is a set of lines with $|L| \ll |B|^2$.

Proof. Let $X = (A+B)^{-1}$ and $S = (1/A + 1/B)^{-1}$. Note that elements of S are of the form $ab/(a+b)$ with $a \in A$ and $b \in B$. Observing the identity

$$\frac{1}{b} - \frac{1}{b^2} \cdot \frac{ab}{a+b} = \frac{1}{a+b},$$

it follows that the cardinality

$$|\{(c, d, s) \in B^{-1} \times B^{-1} \times S : (c - sc^2, d - sd^2) \in X \times X\}| \tag{43}$$

can be interpreted as the number of incidences between $X \times X$ and the set of $O(|B|^2)$ lines of the form

$$y = \frac{d^2}{c^2}x + d\Big(1 - \frac{d}{c}\Big). \tag{44}$$

Furthermore, note that if a quadruple $(a_1, a_2, b_1, b_2) \in A^2 \times B^2$ satisfies

$$\frac{1}{a_1} + \frac{1}{b_1} = \frac{1}{a_2} + \frac{1}{b_2},$$

then $(b_1^{-1}, b_2^{-1}, a_1 b_1/(a_1 + b_1))$ is a unique solution to (43). □

4. Proofs of the Main Results

4.1. Incidence Bounds

Proof of Theorem 1. First, we collect some useful tools that will be required in the proof of Theorem 1. Claim 1, stated below, closely follows [12, Claims 1 and 2]. Although, by carrying out some calculations more efficiently, we obtain an improvement on the final conclusion of this result.

Claim 1. *Let $A, B \subseteq \mathbb{F}_q$ and let $T = T^*(A, B)$ defined in (7). There exist distinct elements $b_1, b_2 \in B$ and a set $C \subset (B - b_1)/(b_2 - B)$ with*

$$|C| \gg \frac{T^5}{|A|^{10}|B|^{14}} \tag{45}$$

such that for all $c \in C$, there exist subsets $A_1^{(c)}, A_2^{(c)} \subseteq A$ with

$$|A_1^{(c)}|, |A_2^{(c)}| \gg \frac{T}{|A||B|^3} \tag{46}$$

satisfying

$$|A_1^{(c)} + cA_2^{(c)}| \ll \frac{|A|^{11}|B|^{15}}{T^5} \tag{47}$$

and

$$|A_2^{(c)} + A_2^{(c)}| \ll \frac{|A|^{23}|B|^{33}}{T^{11}}. \tag{48}$$

Moreover, there exists some $c_* \in C$ such that, writing A_i^* instead of $A_i^{(c_*)}$, for all $c \in C$ we have

$$|A_1^{(c)} \cap A_1^*||A_2^{(c)} \cap A_2^*| \gg \frac{T^4}{|A|^6|B|^{12}} \tag{49}$$

and

$$|c_*A_2^* + cA_2^*| \ll \frac{|A|^{51}|B|^{75}}{T^{25}}. \tag{50}$$

Proof. By the pigeonhole principle, there exist distinct elements $b_1, b_2 \in B$ such that

$$\left|\left\{(a_1, a_2, b) \in \ A \times A \times B : a_1\Big(1 - \frac{b - b_1}{b_2 - b_1}\Big) + a_2\Big(\frac{b - b_1}{b_2 - b_1}\Big) \in A\right\}\right| \gg \frac{T}{|B|^2}.$$

By Lemma 13, there exists a set $B^{'} \subseteq B \setminus \{b_1, b_2\}$, with $|B^{'}| \gg T/(|A|^2|B|^2)$, such that for each $b \in B^{'}$ there exist $\Omega(T/|B|^3)$ pairs $(a_1, a_2) \in A \times A$, which satisfy

$$a_1\Big(1 - \frac{b - b_1}{b_2 - b_1}\Big) + a_2\Big(\frac{b - b_1}{b_2 - b_1}\Big) \in A.$$

For $b \in B^{'}$ denote

$$G = \left\{(a_1, a_2) \in A^2 : a_1\Big(1 - \frac{b - b_1}{b_2 - b_1}\Big) + a_2\Big(\frac{b - b_1}{b_2 - b_1}\Big) \in A\right\},$$

such that $|G| \gg T/|B|^3$. We apply Lemma 11 with

$$X = \Big(1 - \frac{b - b_1}{b_2 - b_1}\Big)A, \quad Y = \Big(\frac{b - b_1}{b_2 - b_1}\Big)A.$$

Consequently, we deduce that there exist subsets $A_1^{(b)}, A_2^{(b)} \subseteq A$, with

$$|A_1^{(b)}|, |A_2^{(b)}| \gg \frac{T}{|A||B|^3},$$

which satisfy

$$\left|A_1^{(b)} + \frac{b - b_1}{b_2 - b}A_2^{(b)}\right| \ll \frac{|A|^{11}|B|^{15}}{T^5}.$$

Let

$$C^{'} = \left\{\frac{b - b_1}{b_2 - b} : b \in B^{'}\right\}$$

and note that

$$|C^{'}| \approx |B^{'}| \gg \frac{T}{|A|^2|B|^2}.$$

Then for each $c \in C^{'}$, by a change of the indexing, we have sets $A_1^{(c)}, A_2^{(c)} \subset A$, with

$$|A_1^{(c)} + cA_2^{(c)}| \ll \frac{|A|^{11}|B|^{15}}{T^5}$$

and

$$|A_1^{(c)}|, |A_2^{(c)}| \gg \frac{T}{|A||B|^3}.$$

This gives (46) and (47). Let $P_c = A_1^{(c)} \times A_2^{(c)}$. Then, for each $c \in C^{'}$, it follows that

$$|P_c| \gg \frac{T^2}{|A|^2|B|^6}.$$

By the Cauchy-Schwarz inequality, we have

$$|C^{'}|\frac{T^2}{|A|^2|B|^6} \ll \sum_{c\in C^{'}} |P_c| \leq |A|\Big(\sum_{c_1,c_2\in C^{'}} |P_{c_1} \cap P_{c_2}|\Big)^{1/2}.$$

Then, by the pigeonhole principle, there exists $c_* \in C^{'}$ such that

$$\sum_{c\in C^{'}} |P_c \cap P_{c_*}| \gg |C^{'}|\frac{T^4}{|A|^6|B|^{12}} \gg \frac{T^5}{|A|^8|B|^{14}}.$$

By Lemma 13, there exists a subset $C \subseteq C^{'}$, with

$$|C| \gg \frac{T^5}{|A|^{10}|B|^{14}},$$

such that for each $c \in C$

$$|P_c \cap P_{c_*}| \gg \frac{T^4}{|A|^6|B|^{12}}.$$

This implies (49), since

$$|P_c \cap P_{c_*}| = |A_1^{(c)} \cap A_1^*||A_2^{(c)} \cap A_2^*|.$$

By Lemma 8, (46) and (47) we get

$$|A_2^{(c)} + A_2^{(c)}| \leq \frac{|A_1^{(c)} + cA_2^{(c)}|^2}{|A_2^{(c)}|} \ll \frac{|A|^{23}|B|^{33}}{T^{11}},$$

which proves (48). Next, by Lemma 8, we have

$$|c_*A_2^* + cA_2^{(c)}| \leq \frac{|c_*A_2^* + (A_1^{(c)} \cap A_1^*)||cA_2^{(c)} + (A_1^{(c)} \cap A_1^*)|}{|A_1^{(c)} \cap A_1^*|}$$
$$\leq \frac{|A_1^* + c_*A_2^*||A_1^{(c)} + cA_2^{(c)}|}{|A_1^{(c)} \cap A_1^*|}. \tag{51}$$

Then, by Lemma 8 and (51) we get

$$|c_*A_2^* + cA_2^*| \leq \frac{|c_*A_2^* + c(A_2^{(c)} \cap A_2^*)||cA_2^* + c(A_2^{(c)} \cap A_2^*)|}{|A_2^{(c)} \cap A_2^*|}$$
$$\leq \frac{|c_*A_2^* + cA_2^{(c)}||A_2^* + A_2^*|}{|A_2^{(c)} \cap A_2^*|}$$
$$\leq \frac{|A_1^* + c_*A_2^*||A_1^{(c)} + cA_2^{(c)}||A_2^* + A_2^*|}{|A_1^{(c)} \cap A_1^*||A_2^{(c)} \cap A_2^*|}.$$

We obtain (50) by applying (47), (48) and (49). □

We use Lemma 7 and Claim 1 to record a useful covering argument.

Claim 2. *Fix $n \leq 4$ and for $1 \leq i \leq n$, let $c_i \in C$ be arbitrary elements. Let*

$$\Gamma := \frac{|A|^{40}|B|^{60}}{T^{20}}. \tag{52}$$

Given any set $Y \subseteq A_2^*$, there exists a subset $Y' \subseteq Y$ with $|Y'| \approx |Y|$ such that, for $1 \leq i \leq n$, the sets $\pm c_iY'$ can each be fully covered by $O(\Gamma)$ translates of A_1^*.

Proof. Fix $0 < \epsilon < 1/16$. For $1 \leq i \leq n$, by Lemma 7, there exist sets $Y_{c_i} \subseteq Y$ with $|Y_{c_i}| \geq (1-\epsilon)|Y|$ such that $\pm c_iY_{c_i}$ can be covered by

$$O_\epsilon\left(\frac{|\pm c_iY \pm (A_1^{(c_i)} \cap A_1^*)|}{|A_1^{(c_i)} \cap A_1^*|}\right) = O_\epsilon\left(\frac{|c_iA_2^* + (A_1^{(c_i)} \cap A_1^*)|}{|A_1^{(c_i)} \cap A_1^*|}\right)$$

translates of $A_1^{(c_i)} \cap A_1^* \subseteq A_1^*$. Now, for any $c \in C$, using Lemma 8 and the estimates (47), (48) and (49) we get

$$\frac{|cA_2^* + (A_1^{(c)} \cap A_1^*)|}{|A_1^{(c)} \cap A_1^*|} \leq \frac{|cA_2^* + c(A_2^{(c)} \cap A_2^*)||(A_1^{(c)} \cap A_1^*) + c(A_2^{(c)} \cap A_2^*)|}{|A_1^{(c)} \cap A_1^*||A_2^{(c)} \cap A_2^*|}$$
$$\leq \frac{|A_2^* + A_2^*||A_1^{(c)} + cA_2^{(c)}|}{|A_1^{(c)} \cap A_1^*||A_2^{(c)} \cap A_2^*|}$$
$$\ll \frac{|A|^{40}|B|^{60}}{T^{20}}.$$

Let $Y^{'} = Y_{c_1} \cap \cdots \cap Y_{c_n}$, so that $|Y^{'}| \geq (1-n\epsilon)|Y| \geq (3/4)|Y|$. Hence, for $1 \leq i \leq n$, the sets $\pm c_i Y^{'}$ are each fully contained in $O(\Gamma)$ translates of A_1^*. □

We apply Lemma 12 with $X = A_2^*$ and $Y = C/c_*$. Recalling (50), we take

$$M = O\bigg(\frac{|A|^{51}|B|^{75}}{T^{25}}\bigg).$$

Hence, there exist elements $a_1, a_2, a_3 \in A_2^*$ such that

$$\bigg|(A_2^* - a_1) \cap \frac{a_2 - a_3}{c_*}C\bigg| \gg \frac{|A_2^*||C|}{M} \gg \frac{T^{31}}{|A|^{62}|B|^{92}}.$$

Since the conditions and the desired estimates of Theorem 1 are unchanged under dilation, without loss of generality, we assume $(a_2 - a_3) = 1$. Then, setting

$$D = (A_2^* - a_1) \cap (C/c_*),$$

we have

$$|D| \gg \frac{T^{31}}{|A|^{62}|B|^{92}}. \tag{53}$$

We consider three cases.

Case 1: $1 + R(D) \nsubseteq R(D)$. There exist elements a, b, c, $d \in C$ such that

$$r = 1 + \frac{a-b}{c-d} \notin R(D).$$

By Lemma 3, for any set $D^{'} \subseteq D$, with $|D^{'}| \approx |D|$, we have

$$|D^{'}|^2 = |D^{'} + rD^{'}|.$$

Let $E \subseteq A_2^*$ with $|E| \approx |A_2^*|$. Applying Lemma 8 with $X = (c-d)E$, we get

$$\begin{aligned} |E||D^{'}|^2 &\leq |E||(c-d)D^{'} + (c-d)D^{'} + (a-b)D^{'}| \\ &\leq |E + D^{'} + D^{'}||cE - dE + aD^{'} - bD^{'}| \\ &\leq |A_2^* + A_2^* + A_2^*||cE - dE + aD^{'} - bD^{'}|. \end{aligned}$$

Now, by Claim 2, there exist subsets $E^{'} \subseteq A_2^*$ with $|E^{'}| \approx |A_2^*|$ and $D^{''} \subseteq D$ with $|D^{''}| \approx |D|$ such that $cE^{'}, -dE^{'}, aD^{''}, -bD^{''}$ are contained in $O(\Gamma)$ translates of A_1^*. Thus, setting $E = E^{'}$ and $D^{'} = D^{''}$, we get

$$|A_2^*||D|^2 \ll \Gamma^4 |A_2^* + A_2^* + A_2^*||A_1^* + A_1^* + A_1^* + A_1^*|.$$

By Lemma 8, it follows that

$$|D|^2 \ll \Gamma^4 \frac{|A_1^* + c_* A_2^*|^7}{|A_1^*|^2|A_2^*|^4}.$$

We use (46), (47), (52) and (53) to conclude

$$T^{183} \ll |A|^{367}|B|^{547}.$$

Case 2: $D \cdot R(D) \nsubseteq R(D)$. There exist elements a, b, c, d, $e \in C$ such that

$$r = \frac{a}{c_*}\frac{b-c}{d-e} \notin R(D).$$

Then, for any subset $D^{'} \subseteq D$, with $|D^{'}| \approx |D|$, by Lemma 3, we have

$$|D^{'}|^2 = |D^{'} + rD^{'}|.$$

Let $E \subseteq A_2^*$ be any set with $|E| \approx |A_2^*|$. Applying Lemma 8 with $X = \frac{b-c}{d-e}E$, we get

$$\begin{aligned} |E||D^{'}|^2 &= |E||D^{'} + rD^{'}| \\ &\leq \Big|D^{'} + \frac{b-c}{d-e}E\Big||c_*E + aD^{'}| \\ &\leq |dD^{'} - eD^{'} + bE - cE||c_*E + aD^{'}|. \end{aligned}$$

By Claim 2, there exist subsets $D^{''} \subseteq D$ with $|D^{''}| \approx |D|$ and $E^{'} \subseteq E$ with $|E^{'}| \approx |E|$ such that $aD^{''}, dD^{''}, -eD^{''}, bE^{'}, -cE^{'}$ are contained in $O(\Gamma)$ translates of A_1^*. Thus, setting $D^{'} = D^{''}$ and $E = E^{'}$, we get

$$\begin{aligned} |A_2^*||D|^2 &\ll \Gamma^5|A_1^* + A_1^* + A_1^* + A_1^*||A_1^* + c_*A_2^*| \\ &\ll \Gamma^5\frac{|A_1^* + c_*A_2^*|^5}{|A_2^*|^3}. \end{aligned}$$

To obtain the last inequality we used Lemma 8. Then, by (46), (47), (52) and (53), we get

$$T^{191} \ll |A|^{383}|B|^{571}.$$

Case 3: Cases 1 and 2 do not happen. Thus, by Lemma 5 applied to the set D, we have $R(D) = \mathbb{F}_D$. Based on our assumption on the set A, we consider three cases.
Case 3.1: $R(D) = \mathbb{F}_q$ and $|D| > q^{1/2}$. Let Y be an arbitrary subset of D with $|Y| \approx |D|$. Then, by Lemma 6, there exists an element $\xi \in \mathbb{F}_q^* \subset R(D)$ such that $q \ll |Y + \xi Y|$. Since $\xi \in R(D)$, there exist elements $a, b, c, d \in C$ such that

$$q \ll |aY - bY + cY - dY|. \tag{54}$$

By Claim 2, there exists a subset $D^{'} \subseteq D$, with $|D^{'}| \approx |D|$ such that $aD^{'}$, $-bD^{'}$, $cD^{'}$ and $-dD^{'}$ can be covered by $O(\Gamma)$ translates of A_1^*. We set $Y = D^{'}$, so that by (54) and Lemma 8, we get

$$q \ll \Gamma^4|A_1^* + A_1^* + A_1^* + A_1^*| \ll \Gamma^4\frac{|A_1^* + c_*A_2^*|^4}{|A_2^*|^3}.$$

Then, by (46), (47), (52) and (53), we conclude that

$$T^{103} \ll q^{-1}|A|^{207}|B|^{309}.$$

Moreover, by Lemma 4, the assumption $|D| > q^{1/2}$ implies that $R(D) = \mathbb{F}_q$. Hence, if $|D| > q^{1/2}$ then all other cases become impossible.

Case 3.2: Either $R(D) = \mathbb{F}_q$ and $|D| \leq q^{1/2}$ or $R(D)$ is a proper subfield and $|D| = |D \cap R(D)| \ll |R(D)|^{1/2}$. Let Y be an arbitrary subset of D with $|Y| \approx |D|$. By Lemma 6, there exist elements $a, b, c, d \in C$ such that

$$|D|^2 \ll |aY - bY + cY - dY|. \tag{55}$$

By Claim 2, there exists a subset $D^{'} \subseteq D$, with $|D^{'}| \approx |D|$ such that $aD^{'}$, $-bD^{'}$, $cD^{'}$ and $-dD^{'}$ can be covered by $O(\Gamma)$ translates of A_1^*. We set $Y = D^{'}$, so that by (55) and Lemma 8 we get

$$|D|^2 \ll \Gamma^4|A_1^* + A_1^* + A_1^* + A_1^*| \ll \Gamma^4 \frac{|A_1^* + c_* A_2^*|^4}{|A_2^*|^3}.$$

Then, by (46), (47), (52) and (53), we conclude the inequality

$$T^{165} \ll |A|^{331}|B|^{493}.$$

Case 3.3: $R(D)$ is a proper subfield and

$$|D| = |D \cap R(D)| \ll |A|^{31/191}|B|^{129/191}.$$

Then, by (53), we obtain

$$T^{191} \ll |A|^{383}|B|^{571}.$$

Finally, collecting the acquired bounds on $T^*(A, B)$ from the above cases, we use (8) to conclude estimate (9). Then, we get (10) and (11) by subbing the acquired bound on $T(A, B)$ into the inequalities (38) and (39) respectively. □

Proof of Theorem 2. Let $A, B \subset \mathbb{F}_q$ and let $T = T^*(A, B)$. Throughout the proof, we treat A and B as potentially different sets. However, our method is not particularly effective in dealing with sets of different sizes and so ultimately we assume $|A| = |B|$ to prove estimate (13) under restriction (12).

By the pigeonhole principle, there exist distinct elements $b_1, b_2 \in B$ such that

$$\left|\left\{(a_1, a_2, b) \in \ A \times A \times B : a_1\Big(1 - \frac{b - b_1}{b_2 - b_1}\Big) + a_2\Big(\frac{b - b_1}{b_2 - b_1}\Big) \in A\right\}\right| \gg \frac{T}{|B|^2}.$$

Let

$$B_* = \left\{\frac{b - b_1}{b_2 - b_1} : b \in B \setminus \{b_1\}\right\}.$$

By Lemma 13 there exists a set $A_* \subseteq A$, with $|A_*| \gg T/(|A||B|^3)$, such that

$$|\{(a_1, a_2, b) \in A \times A_* \times B_* : a_1(1-b) + a_2 b \in A\}| \gg \frac{T}{|B|^2} \tag{56}$$

and for each $a \in A_*$ we have

$$|\{(a_1, b) \in A \times B_* : a_1(1-b) + ab \in A\}| \gg \frac{T}{|A||B|^2}. \tag{57}$$

By the pigeonhole principle, applied to (56), there exists an element $b_0 \in B_*$ such that

$$\left|\{(a_1, a_2) \in A \times A_* : a_1(1-b_0) + a_2 b_0 \in A\}\right| \gg \frac{T}{|B|^3}. \tag{58}$$

We apply Lemma 10 with

$$X = b_0 A_*, \quad Y = (b_0 - 1)A \quad \text{and} \quad G = \{(x, y) \in X \times Y : x - y \in A\}.$$

Observing that

$$|X| \leq |A|, \quad |Y| = |A|, \quad |G| \gg \frac{T}{|B|^3} \quad \text{and} \quad |X \overset{G}{-} Y| \leq |A|,$$

we deduce that there exists a subset $A^{'} \subseteq A_*$, with

$$|A'| \gg \frac{|G|}{|Y|} \gg \frac{T}{|A||B|^3}, \tag{59}$$

such that

$$|A' - A'| \ll \frac{|X \overset{G}{-} Y|^4 |X|^4 |Y|^3}{|G|^5} \ll \frac{|A|^{11}|B|^{15}}{T^5}. \tag{60}$$

Since $A' \subseteq A_*$, by (57) and (59), it follows that

$$|\{(a_1, a_2, b) \in A \times A^{'} \times B_* : a_1(1-b) + a_2 b \in A\}| \gg \frac{T^2}{|A|^2|B|^5}. \tag{61}$$

By the pigeonhole principle, applied to (61), there exists an element $a_0 \in A$ such that

$$|\{(a, b) \in A^{'} \times B_* : a_0(1-b) + ab \in A\}| \gg \frac{T^2}{|A|^3|B|^5}.$$

Equivalently,

$$|\{(a, b) \in (A^{'} - a_0) \times B_* : ab \in (A - a_0)\}| \gg \frac{T^2}{|A|^3|B|^5}. \tag{62}$$

We use Lemma 10, multiplicatively, with

$$X = A^{'} - a_0, \quad Y = B_*^{-1} \quad \text{and} \quad G = \{(x, y) \in X \times Y : x/y \in (A - a_0)\}.$$

Observe that

$$|X| \leq |A|, \quad |Y| \approx |B|, \quad |G| \gg \frac{T^2}{|A|^3|B|^5} \quad \text{and} \quad |\overset{G}{X/Y}| \leq |A|.$$

We conclude that there exists a subset $C \subseteq A^{'} - a_0$, with

$$|C| \gg \frac{|G|}{|Y|} \gg \frac{T^2}{|A|^3|B|^6}, \tag{63}$$

such that

$$|C/C| \ll \frac{|\overset{G}{X/Y}|^4|X|^4|Y|^3}{|G|^5} \ll \frac{|A|^{23}|B|^{28}}{T^{10}}. \tag{64}$$

Since $C \subseteq A' - a_0$, by (60), we also have

$$|C - C| \ll \frac{|A|^{11}|B|^{15}}{T^5}. \tag{65}$$

By Lemma 1, applied to the set C, we get

$$T^*(A, B) \ll |A|^{217/104}|B|^{302/104} + q^{-1/95}|A|^{199/95}|B|^{277/95}.$$

To obtain (13), we set $B = A$ and use (8). It remains to justify our use of Lemma 1. Fix an arbitrary $0 < \eta < 1/8$. Then, for any constant $\lambda > 0$, we may assume $\lambda|A|^{51/52} \leq \eta|C|$ as otherwise, recalling (63), we can use the lower bound $|C| \gg T^2/|A|^9$ to obtain the required estimate. Now, suppose the set A satisfies condition (12). Then, given an arbitrary proper subfield G and element $c \in \mathbb{F}_q$, there exists some constant $\lambda > 0$ such that

$$|C \cap cG| \leq |(A - a_0) \cap cG| \leq \lambda \cdot \max\{|G|^{1/2}, |A|^{51/52}\} \leq \max\{\lambda|G|^{1/2}, \eta|C|\},$$

as required. Finally, we obtain (14) and (15) by subbing the acquired bound on $T(A)$ into the inequalities (38) and (39) respectively. □

Proof of Theorem 3. Recall the definitions (5) and (33). The number of collinear triples formed by $A \times A$ can be expressed as

$$T(A) = \sum_{a,b \in A} E_{\times}(A - a, A - b).$$

By (34) and another application of the Cauchy-Schwarz inequality, we get

$$T(A) \leq \left(\sum_{a \in A} E_{\times}(A - a)^{1/2} \right)^2 \leq |A| \sum_{a \in A} E_{\times}(A - a) \leq |A|^2 \max_{a \in A} E_{\times}(A - a).$$

Then, under restriction (18), we can bound $\max_{a \in A} E_{\times}(A - a)$ using Lemma 2. This concludes the proof of (19). □

Proof of Corollary 1. Under restriction (18), with $\delta = 2/5$, we use (19) and the assumption $|A + A| \approx |A|$ to get (21). Then, using this bound on $T(A)$ together with (38) and (39), we obtain the estimates (22) and (23) respectively. □

4.2. Applications

Proof of Corollary 2. We use Lemma 15, together with the incidence bound (14) of Theorem 2, to deduce (25). Then, we set $B = A$ and apply (41) to get

$$\frac{|A|^4}{|1/A + 1/A|} \ll \left(|A + A|^{173/104} + q^{-1/285}|A + A|^{476/285}\right)|A|^{4/3}.$$

Hence, either

$$|A + A|^{519}|1/A + 1/A|^{312} \gg |A|^{832}$$

or

$$|A + A|^{476}|1/A + 1/A|^{285} \gg q|A|^{760}.$$

This gives (26). Next, we set $B = A^{-1}$ and use (41) to get

$$\frac{|A|^4}{|A + 1/A|} \ll \left(|A + 1/A|^{173/104} + q^{-1/285}|A + 1/A|^{476/285}\right)|A|^{4/3},$$

which gives estimate (27).

Now, assume that $\mathbb{F}_q$ does not contain any proper subfields G, with

$$|A|^{51/52} < |G| < |A|^{(2\cdot 832)/831}. \tag{66}$$

Then, suppose that for some proper subfield G and elements $c, d \in \mathbb{F}_q$, the left hand side of (24) is larger than $|G|^{1/2}$. By our assumption (66), either $|G| \le |A|^{51/52}$ so that restriction (24) is satisfied or $|G| \ge |A|^{(2\cdot 832)/831}$ so that we have

$$|A + B| \ge |G|^{1/2} \ge |A|^{1+1/831}.$$

This gives the relevant required estimates for both cases $B = A$ and $B = A^{-1}$. Finally, we restate (66) as a condition on A, by asking that the cardinality of A does not lie in the intervals $(|G|^{1/2-1/1664}, |G|^{1+1/51})$ for all proper subfields G of $\mathbb{F}_q$. □

Proof of Corollary 3. Let $S = A \cap \alpha/A$. Suppose that S satisfies condition (24). Then, noting that $S + S \subseteq A + A$ and $\alpha/S + \alpha/S \subseteq A + A$, by the estimate (26) we have

$$|S| \ll |A + A|^{831/832} + q^{-1/760}|A + A|^{761/760}.$$

Now, suppose that for all proper subfields G and elements $c, d \in \mathbb{F}_q$ we have

$$|(A + A)^{-1} \cap (cG + d)| \ll \max\{|G|^{1/2}, |A + A|^{(831\cdot 51)/(832\cdot 52)}\}. \tag{67}$$

It follows that either $|S| < |A + A|^{831/832}$, which gives the desired result or, by (67), we can deduce that S satisfies condition (24). Finally, note that $47/48 < (831\cdot 51)/(832\cdot 52)$, which means that condition (67) is satisfied under condition (28).

Suppose that for all proper subfields $G \subset \mathbb{F}_q$, $|A| \notin (|G|^{1/2-1/1664}, |G|^{1+1/47})$. Hence $\mathbb{F}_q$ does not contain any proper subfields G with

$$|A|^{47/48} < |G| < |A|^{(2\cdot 832)/831}.$$

Then if, for some $c, d \in \mathbb{F}_q$ and a proper subfield G, the left hand side of (67) is larger than $|G|^{1/2}$, it follows that either $|G| \leq |A|^{47/48}$ so that (28) is satisfied or

$$|A+A| \geq |G|^{1/2} \geq |A|^{832/831} \geq |S|^{832/831},$$

which gives the required estimate. □

Proof of Corollary 4. Let $X = (A+A)^{-1} = 1/A$ and let L be any set of lines. Note that, using estimate (19) together with (38), we can bound $I(X \times X, L)$ in terms of $|X+X|$. We use identity (42) of Lemma 15, as well as (41), to deduce

$$\begin{aligned}\frac{|A|^4}{|1/A+1/A|} \leq & E_+(1/A) \ll (\log|A|)^{1/3} \cdot \big(|1/A+1/A|^{7/12}|A| + |A|^{5/3-\delta/6} \\ & + |1/A+1/A|^{6/15}|A|^{18/15} + |1/A+1/A|^{7/12}|A|^{7/6}q^{-1/12}\big)|A|^{4/3}.\end{aligned}$$

Choosing $\delta = 2/7$, we obtain the required result based on the last three terms of the above inequality and note that the first term yields a better bound than required. Given this choice of δ, by (18), we see that (30) gives the necessary restriction on A^{-1}. Finally, if we assume that there are no proper subfields with

$$|A|^{5/7} < |G| < |A|^2,$$

then it follows that restriction (30) is satisfied for all proper subfields. Since (30) fails only if there exist some elements $c, d \in \mathbb{F}_q$ and a proper subfield G such that

$$|A| \geq |A^{-1} \cap (cG+d)| > |G|^{1/2} \geq |A|,$$

which is impossible. This concludes the proof of the required lower bound on $|1/A+1/A|$. A similar argument gives the same bound for $|1/A-1/A|$. To see this note that when applying (19) and (41), one may replace $X+X$ by $X-X$. □

Acknowledgments. The author would like to thank Simon Macourt and Igor Shparlinski for their helpful comments.

References

[1] E. Aksoy Yazici, B. Murphy, M. Rudnev and I. D. Shkredov, Growth estimates in positive characteristic via collisions, *Int. Math. Res. Not. IMRN* **2017**(23) (2017), 7148-7189.

[2] J. Bourgain, More on the sum-product phenomenon in prime fields and its applications, *Int. J. Number Theory* **1**(1) (2005), 1-32.

[3] J. Bourgain, Multilinear exponential sums in prime fields under optimal entropy condition on the sources, *Geom. Funct. Anal.* **18**(5) (2009), 1477-1502.

[4] J. Bourgain and M. Z. Garaev, On a variant of sum-product estimates and explicit exponential sum bounds in prime fields, *Math. Proc. Cambridge Philos. Soc.* **146**(1) (2009), 1-21.

[5] J. Bourgain and M. Z. Garaev, Sumsets of reciprocals in prime fields and multilinear Kloosterman sums, *Izv. Ross. Akad. Nauk Ser. Mat.* **78**(4) (2014), 19-72; translation in *Izv. Math.* **78** (2014), 656-707.

[6] J. Bourgain and A. Glibichuk, Exponential sum estimates over a subgroup in an arbitrary finite field, *J. Anal. Math.* **115** (2011), 51-70.

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

[8] J. Cilleruelo and M. Z. Garaev, Concentration of points on two and three dimensional modular hyperbolas and applications, *Geom. Funct. Anal.* **21**(4) (2011), 892-904.

[9] G. Elekes, Sums versus products in number theory, algebra and Erdős geometry, Paul Erdős and his mathematics II, *Bolyai Soc. Math. Stud.* **11** (2002), 241-290.

[10] M. Z. Garaev, The sum-product estimate for large subsets of prime fields, *Proc. Amer. Math. Soc.* **136** (2008), 2735-2739.

[11] H. A. Helfgott and M. Rudnev, An explicit incidence theorem in $\mathbb{F}_p$, *Mathematika* **57**(1) (2011), 135-145.

[12] T. G. F. Jones, Explicit incidence bounds over general finite fields, *Acta Arith.* **150**(3) (2011), 241-262.

[13] T. G. F. Jones, An improved incidence bound for fields of prime order, *European J. Combin.* **52** (2016), 136-145.

[14] N. H. Katz and C.-Y. Shen, A slight improvement to Garaev's sum product estimate, *Proc. Amer. Math. Soc.* **136**(7) (2008), 2499-2504.

[15] N. H. Katz and C.-Y. Shen, Garaev's inequality in finite fields not of prime order, *Online J. Anal. Comb.* **3** (2008), Article 3.

[16] L. Li and O. Roche-Newton, An improved sum-product estimate for general finite fields, *SIAM J. Discrete Math.* **25**(3) (2011), 1285-1296.

[17] S. Macourt and I.E. Shparlinski, Double sums of Kloosterman sums in finite fields; arXiv:1903.10070v1 [math.NT] (to appear in *Finite Fields Appl.*).

[18] B. Murphy and G. Petridis, A point-line incidence identity in finite fields, and applications, *Mosc. J. Comb. Number Theory* **6**(1) (2016), 64-95.

[19] B. Murphy, G. Petridis, O. Roche-Newton, M. Rudnev and I. D. Shkredov, New results on sum-product type growth over fields, *Mathematika* **65**(3) (2019), 588-642.

[20] O. Roche-Newton, Sum-ratio estimates over arbitrary finite fields; arXiv:1407.1654v1 [math.CO].

[21] M. Rudnev, On the number of incidences between planes and points in three dimensions, *Combinatorica* **38**(1) (2018), 219-254.

[22] M. Rudnev, Point-plane incidences and some applications in positive characteristic; arXiv:1806.03534v1 [math.CO].

[23] C.-Y. Shen, An extension of Bourgain and Garaev's sum-product estimates, *Acta Arith.* **135**(4) (2008), 351-356.

[24] I. D. Shkredov, On asymptotic formulae in some sum-product questions, *Trans. Moscow Math. Soc.* **2018** (2018), 231-281.

[25] S. Stevens and F. de Zeeuw, An improved point-line incidence bound over arbitrary fields, *Bull. London Math. Soc.* **49**(5) (2017), 842–858.

[26] E. Szemerédi and W. T. Trotter, Extremal problems in discrete geometry, *Combinatorica* **3**(3–4) (1983), 381-392.

[27] T. Tao and V. Vu, Additive Combinatorics, *Cambridge Univ. Press*, Cambridge, 2006.

[28] L. Vinh, Szemerédi-Trotter type theorems and sum-product estimates in finite fields, *European J. Combin.* **32** (2011), 1177-1181.

Appendix: Proofs of Lemma 1 and Lemma 2

Proof of Lemma 1. Fix some $\epsilon = \epsilon(\eta)$ satisfying

$$\eta < (1-\epsilon)/8 < 1/8. \tag{68}$$

We apply Lemma 9 to identify some subset $B \subseteq A$ with

$$|B| \geq (1-\epsilon)|A|, \tag{69}$$

such that

$$|B+B+B+B| \ll_\epsilon \frac{|A+A|^3}{|A|^2}. \tag{70}$$

We point out that in order to prove the estimates of Lemma 1 involving the difference set $A-A$ instead of the sum set $A+A$, by an alternative use of Lemma 9, one can identify some subset $B^{'} \subseteq A$ with $|B^{'}| \geq (1-\epsilon)|A|$ such that

$$|B^{'}-B^{'}-B^{'}-B^{'}| \ll_\epsilon \frac{|A-A|^3}{|A|^2}. \tag{71}$$

For $X \subseteq \mathbb{F}_q$ and $\xi \in X/X$, we write $r_X(\xi) = |\{(a,b) \in X^2 : b/a = \xi\}|$. Note that

$$\sum_{\xi \in B/B} r_B(\xi) = |B|^2.$$

Let $Y \subseteq B/B$ be the set of popular slopes such that for $\xi \in Y$ we have

$$r_B(\xi) \geq \frac{|B|^2}{2|B/B|}$$

and let $P = \{(x,y) \in B \times B : y/x \in Y\}$. By Lemma 13 with $X = B/B$ and $f = r_B$, it follows that

$$|P| = \sum_{\xi \in Y} r_B(\xi) \geq \frac{|B|^2}{2}.$$

By the pigeonhole principle, there exists some $x_* \in B$, such that the set

$$B_{x_*} = \{y : (x_*, y) \in P\}$$

has cardinality $|B_{x_*}| \geq |B|/2$. For $\xi \in \mathbb{F}_q$, we write $P_\xi = \{x : (x, \xi x) \in P\}$. Then, for all $y \in B_{x_*}$, we have

$$|P_{y/x_*}| = r_B(y/x_*) \geq \frac{|B|^2}{2|B/B|} \quad \text{and} \quad \frac{y}{x_*} P_{y/x_*} \subseteq B. \tag{72}$$

By Lemma 13, with $X = B_{x_*}/B_{x_*}$ and $f = r_{B_{x_*}}$, there exists $S \subseteq B_{x_*} \times B_{x_*}$, with

$$|S| \geq \frac{|B_{x_*}|^2}{2} \geq \frac{|B|^2}{8},$$

such that if $(x, y) \in S$, then

$$r_{B_{x_*}}(y/x) \geq \frac{|B_{x_*}|^2}{2|B_{x_*}/B_{x_*}|} \geq \frac{|B|^2}{8|B/B|}.$$

By the pigeonhole principle there exists a popular abscissa x_0, such that the set $B_{x_0} = \{y : (x_0, y) \in S\}$ has cardinality

$$|B_{x_0}| \geq \frac{|B|}{8}. \tag{73}$$

Since the required estimate and the conditions of Lemma 1 are invariant under dilations of the set A, we may assume, without loss of generality, that $x_0 = 1$. Let

$$S_y = \{x : (x, xy) \in S\} \tag{74}$$

and note that for any $y \in B_1$, we have

$$S_y, yS_y \subseteq B_{x_*} \subseteq B \tag{75}$$

and that

$$|S_y| \gg \frac{|B|^2}{|B/B|}. \tag{76}$$

Next, we record a useful consequence of Lemma 7.

Claim 3. *Let $n \leq 4$ and for $1 \leq i \leq n$, let $b_i \in \pm B_1$ be arbitrary elements. Let*

$$\Gamma := O\bigg(\frac{|A+A||A/A|}{|B|^2}\bigg).$$

Then, for any subset $C \subset B$, a further subset $C_1 \subset C$ can be identified, with $|C_1| \approx |C|$, such that all of b_iC_1 are fully covered by $O(\Gamma)$ translates of B.

Proof. By Lemma 7, for any $0 < \delta \leq 1/16$ and $1 \leq i \leq n$, there exist sets $C_{b_i} \subset C$ with $|C_{b_i}| \geq (1-\delta)|C|$ such that $b_iC_{b_i}$ can be covered by

$$O_\delta\bigg(\frac{|b_iC + b_iS_{b_i}|}{|b_iS_{b_i}|}\bigg) = O_\delta\bigg(\frac{|A+A||A/A|}{|B|^2}\bigg) \tag{77}$$

translates of B. We set $C_1 = C_{b_1} \cap \cdots \cap C_{b_n}$. Then, it follows that $|C_1| \geq (1 - n\delta)|C| \geq (3/4)|C|$ and each of b_iC_1 gets fully covered by $O(\Gamma)$ translates of B. □

We remark that by an alternative use of Lemma 7, one may replace $A+A$ in (77) by $A-A$. By this observation and (71), the remainder of the proof may be easily reworked to produce the same estimates involving the difference set.

First, we assume $|A| \ll q^{1/2}$ and consider four cases corresponding to the nature of the quotient set $R(B_1)$.

Case 1: $R(B_1) \neq R(B_{x_*})$. Recall that $B_1 \subseteq B_{x_*}$, which implies that $R(B_1) \subseteq R(B_{x_*})$. Therefore, according to the assumption of this case, there exists some element $r \in R(B_{x_*})$ such that $r \notin R(B_1)$. Since $r \notin R(B_1)$, given an arbitrary subset $Y \subseteq B_1$, by Lemma 3, we have $|Y|^2 = |Y+rY|$. Namely, there exist elements $a,b,c,d \in B_{x_*}$, such that

$$|Y|^2 \leq |cY - dY + aY - bY|. \tag{78}$$

By Lemma 7 and (72), a positive proportion of cB_1 can be covered by at most

$$\frac{|cB_1 + cP_{c/x_*}|}{|P_{c/x_*}|} \ll \frac{|A+A||A/A|}{|B|^2}$$

translates of $cP_{c/x_*} \subset x_*B$. Similarly, a positive proportion of each of $-dB_1$, aB_1 and $-bB_1$ can be covered by $O(\Gamma)$ translates of x_*B.

Proceeding in a similar manner as Claim 3, an appropriate subset $B_1^{'} \subset B_1$ of size $|B_1^{'}| \approx |B_1|$ can be identified, so that $cB_1^{'}$, $-dB_1^{'}$, $aB_1^{'}$ and $-bB_1^{'}$ are each fully covered by $O(\Gamma)$ translates of x_*B. Hence, by (78), with $Y = B_1^{'}$, we deduce

$$|B|^2 \ll \frac{|B+B+B+B||A+A|^4|A/A|^4}{|B|^8}. \tag{79}$$

After applying (70), it follows that

$$|A+A|^7|A/A|^4 \gg_\epsilon |A|^{12}. \tag{80}$$

Case 2: $1 + R(B_1) \nsubseteq R(B_1)$. There exist elements $a,b,c,d \in B_1$, such that

$$r = 1 + \frac{a-b}{c-d} \notin R(B_1) = R(B_{x_*}).$$

Recall the set S_a defined in (74). Let $S_a^{'} \subset S_a$ denote an arbitrary subset with $|S_a^{'}| \approx |S_a|$. Also let $B_1^{'}$ be an arbitrary subset of B_1 with $|B_1^{'}| \approx |B_1|$. By Lemma 9, with $X = (c-d)B_1^{'}$, there exists $B_1^{''} \subseteq B_1^{'}$, with $|B_1^{''}| \approx |B_1^{'}| \approx |B|$, such that

$$\begin{aligned} |B_1^{''} + rS_a^{'}| &\leq |(c-d)B_1^{''} + (c-d)S_a^{'} + (a-b)S_a^{'}| \\ &\ll \frac{|B_1^{'} + S_a^{'}|}{|B_1^{'}|}|(c-d)B_1^{'} + (a-b)S_a^{'}|. \end{aligned} \tag{81}$$

Recalling that $B_1^{''}, S_a^{'} \subset B_{x_*}$, by Lemma 3 and (76), we have

$$|B_1^{''} + rS_a^{'}| = |B_1^{''}||S_a^{'}| \gg \frac{|B|^3}{|A/A|}.$$

Then, by (81), it follows that

$$\frac{|B|^4}{|A/A|} \ll |A+A||cB_1^{'} - dB_1^{'} + aS_a^{'} - bS_a^{'}|. \tag{82}$$

Now, by Claim 3, we can identify positively proportioned subsets $C_1 \subset B_1$ and $C_2 \subset S_a$ such that each of cC_1, $-dC_1$ and $-bC_2$ gets fully covered by $O(\Gamma)$ translates of B. We fix $B_1^{'} = C_1$ and $S_a^{'} = C_2$. Then by (82) and a threefold use of Claim 3 we have

$$|B|^{10} \ll |A/A|^4|A+A|^4|B+B+aS_a^{'}+B|.$$

Observing that $aS_a^{'} \subset B$, then applying (70), we conclude that

$$|A+A|^7|A/A|^4 \gg_\epsilon |A|^{12}.$$

Case 3: $B_1 \cdot R(B_1) \not\subseteq R(B_1)$. There exist elements $a, b, c, d, e, f \in B_1$ such that

$$r = a\frac{c-d}{e-f} \notin R(B_1) = R(B_{x_*}).$$

Given any set $Y_1 \subseteq B_{x_*}$, recalling that $S_a \subset B_{x_*}$, by Lemma 3, we have $|Y_1||S_a| = |Y_1 + rS_a|$. For an arbitrary set Y_2, by Lemma 8 with $X = \frac{c-d}{e-f}Y_2$, we obtain

$$\begin{aligned} |Y_2||Y_1||S_a| &= |Y_2||Y_1 + rS_a| \\ &\leq \Big|Y_1 + \frac{c-d}{e-f}Y_2\Big||aS_a + Y_2| \\ &\leq |eY_1 - fY_1 + cY_2 - dY_2||aS_a + Y_2|. \end{aligned}$$

By Claim 3, there exist positively proportioned subsets $C_1 \subset S_e$ and $C_2 \subset S_c$ such that $-fC_1$ and $-dC_2$ can be covered by $O(\Gamma)$ translates of B. We fix $Y_1 = C_1$ and $Y_2 = C_2$. First, noting that eS_e, aS_a, $cS_c \subset B$, we have

$$|Y_1||Y_2||S_a| \ll |B - fY_1 + B - dY_2||A+A|.$$

Then, the covering argument, together with (76), yields

$$\frac{|B|^6}{|A/A|^3} \ll \frac{|B+B+B+B||A+A|^3|A/A|^2}{|B|^4}.$$

Finally, applying (70), it follows that

$$|A+A|^6|A/A|^5 \gg_\epsilon |A|^{12}.$$

Case 4: Cases 1-3 do not happen. By Lemma 5, it follows that $R(B_1) = \mathbb{F}_{B_1}$. Based on the assumptions of Lemma 1, we consider two cases.
Case 4.1: $|A \cap R(B_1)| \ll |R(B_1)|^{1/2}$. Clearly $B_1 \subseteq \mathbb{F}_{B_1} = R(B_1)$. Hence

$$|B_1|^2 = |B_1 \cap R(B_1)|^2 \leq |A \cap R(B_1)|^2 \ll |R(B_1)|.$$

Thus, by Lemma 6, there exist elements $a, b, c, d \in B_1$ such that for any subset $Y \subseteq B_1$ with $|Y| \approx |B_1|$, we have

$$|B|^2 \approx |Y|^2 \ll |aY - bY + cY - dY|.$$

By Claim 3, there exists a subset $B_1^{'} \subset B_1$, with $|B_1^{'}| \approx |B_1|$, such that $aB_1^{'}$, $-bB_1^{'}$, $cB_1^{'}$ and $-dB_1^{'}$ are each fully contained in $O(\Gamma)$ translates of B. We set $Y = B_1^{'}$, to obtain

$$|B|^2 \ll |B + B + B + B| \frac{|A + A|^4 |A/A|^4}{|B|^8}.$$

Then by (70) we have

$$|A + A|^7 |A/A|^4 \gg_\epsilon |A|^{12}.$$

Case 4.2: $R(B_1)$ is a proper subfield and $|A \cap R(B_1)| \leq \eta |A|$ for some fixed $0 < \eta < 1/8$. In particular, we have

$$|B_1| = |B_1 \cap R(B_1)| \leq |A \cap R(B_1)| \leq \eta |A|.$$

On the other hand, by (68), (69) and (73) we have $|B_1| > \eta |A|$. Hence this case is impossible.

Finally, suppose that $|A| \geq \eta^{-1} q^{1/2}$. Then, by (68), (69) and (73) we have $|B_1| > q^{1/2}$. By Lemma 4, it follows that $R(B_1) = \mathbb{F}_q$. Let Y denote an arbitrary subset of B_1 with $|Y| \approx |B_1|$. By Lemma 6, there exists an element $\xi \in \mathbb{F}_q^*$ such that $q \ll |Y + \xi Y|$. Since $R(B_1) = \mathbb{F}_q$, there exist elements $a, b, c, d \in B_1$ such that

$$q \ll |aY - bY + cY - dY|.$$

By Claim 3, there exists a positively proportioned subset $B_1^{'} \subset B_1$, such that $aB_1^{'}$, $-bB_1^{'}$, $cB_1^{'}$ and $-dB_1^{'}$ are each fully covered by $O(\Gamma)$ translates of B. We set $Y = B_1^{'}$ to obtain

$$q \ll |B + B + B + B| \frac{|A + A|^4 |A/A|^4}{|B|^8}.$$

By (70), we conclude

$$|A + A|^7 |A/A|^4 \gg_\epsilon q |A|^{10}.$$

□

Sketch of proof of Lemma 2. Following the proof of [16, Theorem 1.4], there exist integers L and N, with $N < |A|$, $LN < |A|^2$ and such that

$$M := LN^2 \gg \frac{E_\times(A)}{\log |A|}. \tag{83}$$

In particular, it follows

$$L, N > \frac{M}{|A|^2}.$$

By [16, Lemma 3.1], there exists a set $\tilde{A}_{x_0} \subset A$ with

$$|\tilde{A}_{x_0}| \gg \frac{LM}{|A|^3} > \frac{M^2}{|A|^5}. \tag{84}$$

Then, based on the nature of the quotient set $R(\tilde{A}_{x_0})$, five cases are considered. Let

$$K = \min\left\{\frac{|A+A|}{|A|}, \frac{|A-A|}{|A|}\right\}.$$

Case 1 and Case 2 lead to the estimate

$$M^4 \ll K^7|A|^{11}, \tag{85}$$

in Case 3 we get

$$M^3 \ll K|A|^8 \tag{86}$$

and Case 4 yields

$$M^5 \ll K^6|A|^{14}. \tag{87}$$

In Case 5, it follows that $R(\tilde{A}_{x_0}) = \mathbb{F}_{\tilde{A}_{x_0}}$. Here we proceed slightly differently from the proof of [16, Theorem 1.4] and split Case 5 into three cases.
`Case 5.1:` $R(\tilde{A}_{x_0}) = \mathbb{F}_q$ and $|\tilde{A}_{x_0}| > q^{1/2}$. Then, Lemma 6 can be used in conjunction with [16, Application 3.2] to obtain the estimate

$$M^4 \ll q^{-1}K^7|A|^{13}. \tag{88}$$

Furthermore, if $|\tilde{A}_{x_0}| > q^{1/2}$ by Lemma 4 it follows that $R(\tilde{A}_{x_0}) = \mathbb{F}_q$. Then, under this assumption, Cases 2-4 become impossible and Case 5.1 becomes the only possibility for Case 5.
`Case 5.2:` Either $R(\tilde{A}_{x_0}) = \mathbb{F}_q$ and $|\tilde{A}_{x_0}| \leq q^{1/2}$ or $R(\tilde{A}_{x_0})$ is a proper subfield and $|A \cap R(\tilde{A}_{x_0})| \ll |R(\tilde{A}_{x_0})|^{1/2}$. This case is dealt with in Case 5 of the proof of [16, Theorem 1.4], where estimate (85) is recovered.
`Case 5.3:` $R(\tilde{A}_{x_0})$ is a proper subfield and $|A \cap R(\tilde{A}_{x_0})| \ll |A|^{1-\delta}$ for some fixed $\delta > 0$. Then, by (84), we have

$$\frac{M^2}{|A|^5} < |\tilde{A}_{x_0}| = |\tilde{A}_{x_0} \cap R(\tilde{A}_{x_0})| \leq |A \cap R(\tilde{A}_{x_0})| \ll |A|^{1-\delta}.$$

This gives

$$M \ll |A|^{3-\delta/2}. \tag{89}$$

Finally, putting together (83), (85), (87), (88) and (89), we obtain the required bound on $E_\times(A)$. Clearly (86) is a stronger bound than required. □