ACTA ARITHMETICA
150.3 (2011)

Explicit incidence bounds over general finite fields

by

TIMOTHY G. F. JONES (Bristol)

Preliminary notation. This paper uses the following notation throughout. Given two real-valued functions f, g with domain D, we write

- $f \ll g$ or $f = O(g)$ if there is a constant γ such that $f(x) \leq \gamma g(x)$ for all $x \in D$. The implicit constant γ may be different each time this notation is used.
- $f \approx g$ if $f \ll g$ and $g \ll f$.

Given two sets $A, B \subseteq \mathbb{F}_q$, we define:

- the *sumset* $A + B = \{a + b : a \in A, b \in B\}$,
- the *product set* $A \cdot B = \{ab : a \in A, b \in B\}$,
- the *ratio set* $\frac{A}{B} = \{ab^{-1} : a \in A, b \in B, b \neq 0\}$.

1. Introduction

1.1. Incidences. This paper is about incidences between points and lines in a plane. A point is *incident* to a line if it lies on that line, and a single point can be incident to more than one line if they cross at that point. An established problem is to find upper bounds for the number of incidences between finite sets of points and lines of given cardinality.

Specifically, fix a field F and an integer n, and let P and L be finite sets of points and lines respectively in the plane $F \times F$ with $|P| = |L| = n$. Define

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

to be the cardinality of the set of incidences between P and L. The problem is to establish upper bounds on $I(P, L)$. A straightforward exercise in combinatorics [13] shows that one always has $I(P, L) \ll n^{3/2}$. So non-trivial incidence bounds are those of the form $I(P, L) \ll n^{3/2-\epsilon}$ for positive ϵ.

2010 *Mathematics Subject Classification*: Primary 11B75.
Key words and phrases: incidence, finite field.

DOI: 10.4064/aa150-3-3

1.2. Known bounds. Different bounds are known for different choices of the field F. Things are largely settled in the settings $F = \mathbb{R}$ and $F = \mathbb{C}$. The result $\epsilon = 1/6$ was obtained in these settings, by Szeméredi and Trotter [12] and Tóth [14] respectively. In both cases, the bound holds unconditionally and is sharp up to multiplicative constants.

Much less is known in the finite field setting $F = \mathbb{F}_q$. It is certainly not possible to have a non-trivial bound that holds in all cases, as the trivial bound $I(P, L) \approx n^{3/2}$ is achieved when $P = F \times F$ and L is the set of lines determined by pairs of points in P. So one must impose some extra conditions.

In this setting Vinh [15] obtained $I(P, L) \ll n^2/q + q^{1/2}n$, which gives non-trivial bounds for $n = q^\alpha$ with $1 < \alpha < 2$. For smaller sets in finite fields, explicit bounds are known only when the field is of prime order p. The best-known such result is due to Helfgott and Rudnev [6] who proved $\epsilon \geq 1/10678$ when $n < p$. This result is unlikely to be best-possible, and followed work of Bourgain, Katz and Tao [2] which established the existence of a non-trivial $\epsilon > 0$ so long as $n < p^{2-\delta(\epsilon)}$, but did not quantify it.

1.3. Extending Helfgott–Rudnev to general finite fields. The Helfgott–Rudnev bound is known only in $\mathbb{F}_p$, and so one would like to extend it to general (i.e. not necessarily prime) finite fields $\mathbb{F}_q$. In particular, it would be good to extend it to $\mathbb{F}_{p^2}$, as this is in some respects a finite analogue of $\mathbb{C}$. However, general finite fields can have subfields, and so stronger conditions than just cardinality are required on P. This is because, as with the example above, if K is a subfield of F then the trivial bound $I(P, L) \approx n^{3/2}$ can be achieved when P is the subplane $K \times K$.

It is therefore interesting to find conditions on $P \subseteq \mathbb{F}_q \times \mathbb{F}_q$ for which an explicit Helfgott–Rudnev-type bound holds for any L with $|L| = |P|$. A natural condition to try imposing on P would be to insist that it is "not too close" to being a copy of a subplane, for example by ensuring that its projection onto either the x- or y-axis is "not too close" to a copy of a subfield. However, the currently-known approaches for proving Helfgott–Rudnev-type bounds rely on first applying a projective transformation to P, which could disrupt such a condition. So any condition must, additionally, be preserved by projective transformations.

1.4. Results. We present an incidence result in $\mathbb{F}_q$, which holds so long as P satisfies certain conditions. Informally, these are that the projection $A(P)$ of P onto some coordinate axis has no more than half-dimensional interaction with large subfields G of $\mathbb{F}_q$, where "large" will be defined relative to the cardinality $n = |P|$.

By no more than "half-dimensional interaction", we mean that $A(P)$ does not intersect an affine copy of G in more than $|G|^{1/2}$ places, and intersects no more than $|G|^{1/2}$ distinct translates of G. Since the motivation is that such sets are a long way from being fields, we shall call them "antifields".

DEFINITION 1. Let F be a field and $\lambda > 0$.

(1) Let $A \subseteq F$. Then
   (a) A is a $(1, \lambda)$-*antifield* if $|A \cap (aG + b)| \leq \max\{\lambda, |G|^{1/2}\}$ for all subfields G of F and all $a, b \in F$.
   (b) A is a $(1, \lambda)$-*strong-antifield* if it is a $(1, \lambda)$-antifield and, for every subfield G with $|G| \geq \lambda$, it intersects strictly fewer than $\max\{\lambda, |G|^{1/2}\}/2$ distinct translates $G + b$ of G.

(2) Let $P \subset F \times F$. Then
   (a) P is a $(2, \lambda)$-*antifield* if the set $\{x : (x, y) \in P\}$ is a $(1, \lambda)$-antifield.
   (b) P is a $(2, \lambda)$-*strong-antifield* if the set $\{x : (x, y) \in P\}$ is a $(1, \lambda)$-strong-antifield.

Note that since one can always apply a change of basis, the projection can in fact be onto any vector multiple of $\mathbb{F}_q$.

Parts (1)(a) and (2)(a) of the definition are motivated by work of Katz and Shen [7] generalising sum-product bounds in $\mathbb{F}_p$ to $\mathbb{F}_q$. Parts (1)(b) and (2)(b) are motivated by the need to avoid disruption by projective transformations. A key idea, which shall be seen later, is that certain projective images of a strong antifield will always be antifields.

We are now able to state the result:

THEOREM 1. *There is an absolute constant γ such that if F is a finite field, P and L are sets of points and lines respectively in $F \times F$ with $|P| = |L| = n$, and P is additionally a $(2, \gamma n^{2560/6419})$-strong-antifield, then $I(P, L) \ll n^{3/2 - 1/12838}$.*

1.5. Examples. Most of this paper is concerned with the proof of Theorem 1. But since it is not necessarily obvious that many point sets should satisfy the conditions of the theorem, we shall first show that it is easy to construct examples in the important cases $q = p^2$ and $q = p^4$. This is demonstrated by the following two corollaries; the first demonstrates the requirement for limited interaction with subfields, and the second demonstrates how one can ignore "small" subfields.

COROLLARY 1 (Construction when $q = p^2$). *Let t be a defining element of $\mathbb{F}_{p^2}$ over $\mathbb{F}_p$, so that $\mathbb{F}_{p^2} = \mathbb{F}_p + t\mathbb{F}_p$. Let $P \subseteq \mathbb{F}_{p^2} \times \mathbb{F}_{p^2}$ with $|P| = n$, and define $A = A(P) = \{x : (x, y) \in P\}$. Suppose that $|A| \ll p$ and $A = \bigcup_{j \in J} A_j$ where $J \subseteq \mathbb{F}_p$ with $|J| \ll \max\{p^{1/2}, n^{2560/6419}\}$, and $A_j \subseteq \mathbb{F}_p + jt$ with*

$|A_j| \ll \max\{p^{1/2}, n^{2560/6419}\}$ for each $j \in J$. Then $I(P,L) \ll n^{3/2-1/12838}$ for all sets L of lines in $\mathbb{F}_{p^2} \times \mathbb{F}_{p^2}$ with $|L| = n$.

Proof. We need to show that the hypotheses imply that the subset P is a $(2, \gamma n^{2560/6419})$-strong-antifield. To do this, we first need to show that P is simply a $(2, \gamma n^{2560/6419})$-antifield. Note that the only sets of the form $a\mathbb{F}_p + b$ with $a, b \in \mathbb{F}_{p^2}$ are given by $\mathbb{F}_p + jt$ and $t\mathbb{F}_p + k$, where j, k range over $\mathbb{F}_p$. Note further that $(\mathbb{F}_p + jt) \cap (t\mathbb{F}_p + k) = \{jt + k\}$. We know by assumption that

$$|A \cap (\mathbb{F}_p + jt)| \ll \max\{p^{1/2}, n^{2560/6419}\}$$

for each $j \in \mathbb{F}_p$. Observe that

$$\begin{aligned} |A \cap (t\mathbb{F}_p + k)| &= \sum_{j \in \mathbb{F}_p} |A \cap (t\mathbb{F}_p + k) \cap (\mathbb{F}_p + jt)| \\ &= \#\{j \in \mathbb{F}_p : |A \cap (\mathbb{F}_p + jt)|\} \\ &\le |J| \ll \max\{p^{1/2}, n^{2560/6419}\}. \end{aligned}$$

So we conclude that P is a $(2, \gamma n^{2560/6419})$-antifield. Since $|J| \ll \max\{p^{1/2}, n^{2560/6419}\}$, it is also a $(2, \gamma n^{2560/6419})$-strong-antifield, as required. ∎

Corollary 2 (Construction when $q = p^4$). *Let t be a defining element of $\mathbb{F}_{p^4}$ over $\mathbb{F}_{p^2}$, so that $\mathbb{F}_{p^4} = \mathbb{F}_{p^2} + t\mathbb{F}_{p^2}$. Let $P \subseteq \mathbb{F}_{p^4} \times \mathbb{F}_{p^4}$ with $|P| = n \gg p^{6419/2560}$, and define $A = A(P) = \{x : (x,y) \in P\}$. Suppose that $|A| \ll p^2$ and $A = \bigcup_{j \in J} A_j$ where $J \subseteq \mathbb{F}_{p^2}$ with $|J| \ll \max\{p, n^{2560/6419}\}$, and $A_j \subseteq \mathbb{F}_{p^2} + jt$ with $|A_j| \ll \max\{p, n^{2560/6419}\}$ for each $j \in J$. Then $I(P,L) \ll n^{3/2-1/12838}$ for all sets L of lines in $\mathbb{F}_{p^4} \times \mathbb{F}_{p^4}$ with $|L| = n$.*

Proof. We need to show that the hypotheses imply that the subset P is a $(2, \gamma n^{2560/6419})$-strong-antifield. Note that since $n \gg p^{6419/2560}$, we can ignore the subfield $\mathbb{F}_p$ and need check this only with respect to the subfields $\mathbb{F}_{p^2}$ and $\mathbb{F}_{p^4}$. This checking follows Corollary 1. ∎

2. Structure for proving Theorem 1. The rest of the paper is concerned with proving Theorem 1. This section outlines the structure of the proof. There are two components to this. The first is a key lemma that relates the algebraic and geometric structure of antifields. The second applies this lemma, and a method of Katz and Shen [7], as part of an otherwise technical generalisation of the Helfgott–Rudnev proof.

2.1. The first component: Relating the algebraic and geometric structure of antifields. Recall that we defined both *antifields* and *strong-antifields*, and that Theorem 1 is a statement about strong-antifields. The first component of the proof of Theorem 1 is to relate the algebraic and geometric structure of these objects by showing that under certain projective transformations the image of a strong-antifield is an antifield.

The formal statement is expressed in terms of *cross ratios*. These are projective invariants, which means that they are preserved by projective transformations of a line and so are important in projective geometry.

Definition 2. Let F be a field and let $a, b, c, d \in F$ with $a \neq d$ and $b \neq c$. Then define the *cross ratio* $X(a, b, c, d)$ by

$$X(a, b, c, d) = \frac{(a-b)(c-d)}{(a-d)(c-b)}.$$

We can now state the key lemma:

Lemma 1. *Let $A \subseteq F$ be a $(1, \lambda)$-strong-antifield and let $B \subseteq F$. Suppose there is a cross-ratio-preserving injection $\tau : B \to A$ (i.e. an injection τ for which $X(\tau(b_1), \tau(b_2), \tau(b_3), \tau(b_4)) = X(b_1, b_2, b_3, b_4)$ whenever $b_1, b_2, b_3, b_4 \in B$). Then B is a $(1, \lambda)$-antifield.*

2.2. The second component: Applying the first component in a technical modification of the Helfgott–Rudnev proof. The structure of the second component broadly follows [6]. It begins by applying Lemma 1 in an adaptation of an argument of Bourgain, Katz and Tao [2] to replace L and P with a construction of lines and points of a certain form, at the expense of some incidences and of passing from a strong-antifield to an antifield.

Proposition 1. *Let F be a field, and let P and L be a set of lines and points respectively in $F \times F$ with $|P| = |L| = n$ such that $I(P, L) = n^{3/2-\epsilon}$ for some $\epsilon > 0$. Let $\lambda \geq 0$. Then, if P is a $(2, \lambda)$-strong-antifield there exist:*

(1) *sets $A, B \subseteq F$ with $|A|, |B| \ll n^{1/2+\epsilon}$ and $0 \notin B$,*
(2) *a set L_A of lines through the origin with gradients in A,*
(3) *a set L_B of horizontal (i.e. gradient 0) lines with y-intercepts in B,*
(4) *a $(2, \lambda)$-antifield P^* with $|P^*| \leq n$, the points of which each lie on the intersection of a line in L_A with a line in L_B,*
(5) *a set L^* of lines with $|L^*| \leq n$ and $L_A, L_B \subseteq L^*$,*

such that $I(P^*, L^*) \gg n^{3/2-5\epsilon}$.

Following [6] we then generalise the definition of incidences to collinear k-tuples for any integer k:

Definition 3. Let F be a field. Let P be a finite set of points in $F \times F$ and let L be a finite set of lines in $F \times F$. We define the number of *collinear k-tuples* between P and L, denoted $I_k(P, L)$, by

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

This generalises the definition of incidences because $I(P,L) = I_1(P,L)$. Moreover, the following lemma shows that Hölder's inequality relates incidences to collinear k-tuples:

LEMMA 2. *Let F be a field and $k \in \mathbb{N}$. Let P, L be sets of points and lines in $F \times F$. Then $I_k(P,L) \geq I(P,L)^k/|L|^{k-1}$.*

Proof. Define $f : L \to \mathbb{N}$ by $f(l) = \sum_{p \in P} \delta_{lp}$ where $\delta_{lp} = 1$ if $p \in L$ and 0 otherwise, i.e. $f(l)$ is the number of points in P that are incident to l. Note that $\|f\|_k = I_k(P,L)^{1/k}$. Hölder's inequality implies that $\|f\|_1 \leq \|f\|_k \|1\|_{k/(k-1)}$, which is the same as $I(P,L) \leq I_k(P,L)^{1/k}|L|^{(k-1)/k}$. ∎

Applying Lemma 2 with $k = 3$ reinterprets Proposition 1 as a lower bound on collinear triples:

COROLLARY 3. *With the notation in Proposition 1 and Definition 3, we also have $I_3(P^*, L(P^*)) \gg n^{5/2-15\epsilon}$, where $L(P^*)$ is the set of lines determined by pairs of points in P^*.*

So we have a lower bound on collinear triples in P^*. Separately, the next proposition gives an upper bound on this quantity, which is obtained by combinatorial methods. Its proof uses the method in [7] to adapt the approach in [6].

PROPOSITION 2. *There is an absolute constant γ_1 such that if:*

- *F is a field and A, B are finite subsets of F with $0 \notin B$,*
- *L_A is the set of lines through the origin with gradients lying in A,*
- *L_B is the set of horizontal lines crossing the y-axis at some $b \in B$,*
- *P is a set of points, each lying on the intersection of some line in L_A with some line in L_B,*
- *$T := I_3(P, L(P))$,*
- *P is, additionally, a $\left(2, \frac{\gamma_1 T^{65}}{|A|^{130}|B|^{194}}\right)$-antifield,*

then

$$T \ll \max\left\{|A|^{\frac{643}{321}}|B|^{\frac{961}{321}}, |A|^{\frac{535}{267}}|B|^{\frac{799}{267}}, |A|^{\frac{499}{249}}|B|^{\frac{745}{249}}\right\}.$$

The results collected above then allow us to prove Theorem 1:

Proving Theorem 1 from the propositions. Let $|P| = |L| = n$ with $I(P,L) = n^{3/2-\epsilon}$. If $\epsilon > 1/12838$ then we are already done, so assume that $\epsilon \leq 1/12838$. We shall find a constant γ such that $\epsilon \geq 1/12838$ so long as P is a $(2, \gamma n^{1/2-1299/12838})$-strong-antifield.

So let us suppose that P is a $(2, \gamma n^{1/2-1299/12838})$-strong-antifield, where γ is a constant to be specified. Apply Proposition 1 and Corollary 3 to obtain a $(2, \gamma n^{1/2-1299/12838})$-antifield P^* for which

$$T := I_3(P^*, L(P^*)) \gg n^{5/2-15\epsilon} \tag{1}$$

and for which Proposition 2 is applicable so long as

$$\gamma n^{1/2-1299/12838} \leq \frac{\gamma_1 T^{65}}{|A|^{130}|B|^{194}} \tag{2}$$

where γ_1 is an absolute constant. Note also that

$$|A|, |B| \ll n^{1/2+\epsilon}. \tag{3}$$

Now, since $\epsilon \leq 1/12838$ and combining (1) and (3), we see that there is an absolute constant γ_2 such that

$$n^{1/2-1299/12838} \leq n^{1/2-1299\epsilon} \leq \gamma_2 \frac{T^{65}}{|A|^{130}|B|^{194}}.$$

So we can ensure that (2) holds by taking $\gamma = \gamma_1/\gamma_2$. We therefore have, by Proposition 2,

$$T \ll \max\left\{|A|^{\frac{643}{321}}|B|^{\frac{961}{321}}, |A|^{\frac{535}{267}}|B|^{\frac{799}{267}}, |A|^{\frac{499}{249}}|B|^{\frac{745}{249}}\right\}. \tag{4}$$

Comparing (1) and (4), plugging in (3), and taking logs then yields $\epsilon \geq 1/12838$ as required.

2.3. The rest of this paper. The proof of Theorem 1 will be complete once Propositions 1 and 2 have been established. Lemma 1 is used for proving Proposition 1. The proofs of these three results are the subject of the rest of the paper:

- Section 3 presents the proof of Lemma 1.
- Section 4 presents the proof of Proposition 1.
- Section 5 collects some technical lemmata that will be useful when proving Proposition 2, some with proof and some without.
- Finally, Section 6 presents the proof of Proposition 2.

3. Proving Lemma 1. For a set A, define $X(A) = \{X(a,b,c,d) : a,b,c,d \in A, a \neq d, b \neq c\}$. To prove Lemma 1 we will need the following intermediate result:

LEMMA 3. *Let F be a field. Suppose $A \subseteq F$ and there is a subfield G of F for which $X(A) \subseteq G$. Then either $|A \cap (xG+y)| \leq 2$ for all $x, y \in F$, or there exist $x, y \in F$ such that $A \subseteq xG+y$.*

Proof. We show that if $|A \cap (xG+y)| \geq 3$ then $A \subseteq xG+y$. Let a, b, c be three distinct elements of $A \cap (xG+y)$ and suppose for a contradiction that $A \nsubseteq xG+y$. Then we can find $d \in A$ with $d \notin xG+y$. So we have

$$a = g_1 x + y, \quad b = g_2 x + y, \quad c = g_3 x + y, \quad d = g_4 x + z,$$

where $g_1, g_2, g_3, g_4 \in G$ and $(z-y)/x \notin G$. Moreover, since a, b, c are distinct, we know that g_1, g_2, g_3 are distinct. Finally, we see that $a, b, c \neq d$. We then know by assumption that

$$\frac{(a-b)(c-d)}{(a-d)(c-b)} \in G.$$

But we also have

$$\begin{aligned}\frac{(a-b)(c-d)}{(a-d)(c-b)} &= \frac{x(g_1-g_2)(x(g_3-g_4)+(y-z))}{(x(g_1-g_4)+(y-z))(x(g_3-g_2))} \\ &= \frac{g_1-g_2}{g_3-g_2}\cdot\frac{g_3-g_4+\frac{y-z}{x}}{g_1-g_4+\frac{y-z}{x}}.\end{aligned}$$

Since g_1, g_2 and g_3 are distinct, this means that

$$\frac{g_3-g_4+\frac{y-z}{x}}{g_1-g_4+\frac{y-z}{x}} =: g_5 \in G.$$

We now split into two cases, according to whether or not $g_5 = 1$. If $g_5 = 1$ then we obtain $g_3 = g_1$, which contradicts the fact that these two elements are distinct. If $g_5 \neq 1$ then we obtain

$$\frac{y-z}{x} = \frac{g_5(g_1-g_4)-g_3+g_4}{1-g_5} \in G,$$

which contradicts the fact that $\frac{y-z}{x} \notin G$. Either way, we are done. ∎

Corollary 4. *Let F be a field, G be a subfield of F, $A \subseteq F$ be a $(1,\lambda)$-strong-antifield, and $A' \subseteq A$ be such that $|A'| \geq \max\{\lambda, |G|^{1/2}\}$. Then $X(A') \nsubseteq G$.*

Proof. Suppose that there exists $A' \subseteq A$ with $|A'| \geq \max\{\lambda, |G|^{1/2}\}$ and $X(A') \subseteq G$. Then by Lemma 3, either $A' \subseteq aG + b$ for some $a, b \in F$, or $|A' \cap (aG+b)| \leq 2$ for all $a, b \in F$.

In the former case, we have $A' \subseteq A \cap (aG+b)$ and so $|A \cap (aG+b)| \geq \max\{\lambda, |G|^{1/2}\}$. In the latter case, $|A' \cap (G+b)| \leq 2$ for all distinct translates $G+b$ of G, which means that A' and therefore A intersects at least $\max\{\lambda, |G|^{1/2}\}/2$ such translates.

Either way, we contradict the fact that A is a $(1,\lambda)$-strong-antifield. ∎

We are now in a position to prove Lemma 1.

Proof of Lemma 1. Suppose for a contradiction that there is a subfield G of F and $a, b \in F$ such that $|B \cap (aG+b)| \geq \max\{\lambda, |G|^{1/2}\}$. Let $B' = B \cap (aG+b)$. Then $\tau(B') \subseteq A$ and $|\tau(B')| = |B'| \geq \max\{\lambda, |G|^{1/2}\}$, but also $X(\tau(B')) = X(B') \subseteq G$. This contradicts Corollary 4.

4. Proof of Proposition 1. We will now use Lemma 1 to prove Proposition 1. Recall that for a point p and a line l we define δ_{pl} to be 1 if $p \in l$ and 0 otherwise. We initially follow [2] and [6].

The first step is to show that we may assume every point in P is incident to $\gg n^{1/2-\epsilon}$ and $\ll n^{1/2+\epsilon}$ lines in L. Indeed, let $P_+ = \{p \in P : p \text{ is incident to} \geq 4n^{1/2+\epsilon} \text{ lines } l \in L\}$. Then

$$\begin{aligned} I(P_+, L) &= \sum_{p\in P_+}\sum_{l\in L}\delta_{pl} \leq \frac{1}{4n^{1/2+\epsilon}}\sum_{p\in P_+}\Big(\sum_{l\in L}\delta_{pl}\Big)^2 \\ &= \frac{1}{4n^{1/2+\epsilon}}\sum_{l,l'\in L}\sum_{p\in P_+}\delta_{pl}\delta_{pl'} \leq \frac{n^{3/2-\epsilon}}{2}. \end{aligned}$$

Similarly, let $P_- = \{p \in P : p \text{ is incident to} \leq n^{1/2-\epsilon}/3 \text{ lines } l \in L\}$. Then

$$I(P_-, L) = \sum_{p\in P_-}\sum_{l\in L}\delta_{pl} \leq \sum_{p\in P_-}\frac{n^{1/2-\epsilon}}{3} \leq \frac{n^{3/2-\epsilon}}{3}.$$

So between them P_+ and P_- contribute only five sixths of the $n^{3/2-\epsilon}$ incidences. Without loss of generality we shall discard them and assume from now on that $|P| \leq n$, and that every point $p \in P$ is incident to $\gg n^{1/2-\epsilon}$ and $\ll n^{1/2+\epsilon}$ lines in L.

Let L_1 be the set of "rich" lines in L defined by

$$L_1 = \{l \in L : l \text{ is incident to} \geq n^{1/2-\epsilon}/20 \text{ points } p \in P\}.$$

Let P_1 be the set of points in P that are "bushy" relative to L_1, defined by

$$P_1 = \{p \in P : p \text{ is incident to } \geq n^{1/2-\epsilon}/20 \text{ lines in } L_1\}.$$

We need to check that P_1 is non-empty. Note first that

$$I(P, L\setminus L_1) = \sum_{p\in P}\sum_{l\in L\setminus L_1}\delta_{pl} \leq \sum_{l\in L\setminus L_1}\frac{n^{1/2-\epsilon}}{20} \leq \frac{n^{3/2-\epsilon}}{20}$$

and therefore $I(P, L_1) \gg I(P, L)$. Now note that

$$I(P\setminus P_1, L_1) = \sum_{p\in P\setminus P_1}\sum_{l\in L_1}\delta_{pl} < \sum_{p\in P\setminus P_1}\frac{n^{1/2-\epsilon}}{20} \leq \frac{n^{3/2-\epsilon}}{20}.$$

This means that $I(P_1, L_1) \gg I(P, L_1) \gg I(P, L)$ and so P_1 is certainly non-empty. Now for each $p \in P_1$ let P_p be the set of points in P that are joined to p by a line in L_1. We have

$$|P_p| = \sum_{q\in P}\sum_{l\in L_1}\delta_{pl}\delta_{ql} = \sum_{l\in L_1}\delta_{pl}\sum_{q\in P}\delta_{ql} \gg n^{1/2-\epsilon}\sum_{l\in L_1}\delta_{pl} \gg n^{1-2\epsilon}.$$

This means that

$$|P_1|n^{1-2\epsilon} \ll \sum_{p\in P_1}|P_p| \leq \sqrt{|P_1|}\sqrt{\sum_{p,q\in P_1}|P_p\cap P_q|}$$

where the second inequality follows by Cauchy–Schwarz. So we have

$$|P_1|n^{2-4\epsilon} \ll \sum_{p,q\in P_1} |P_p \cap P_q|. \tag{5}$$

For each $p \in P$ define x_p to be the x-coordinate of p, and for each $x \in F$ define $P^x = \{p \in P : x_p = x\}$. It is easy to see that $|P^x|n^{1/2-\epsilon} \ll I(P^x, L) \leq 2n$ and so $|P^x| \ll n^{1/2+\epsilon}$ for every $x \in F$. Plugging this into (5) yields

$$\begin{aligned}|P_1|n^{2-4\epsilon} &\ll \sum_{p,q\in P_1 :\, x_p\neq x_q} |P_p \cap P_q| + \sum_{p\in P_1} \sum_{q\in P^{x_p}} |P_p \cap P_q| \\ &\ll \sum_{p,q\in P_1 :\, x_p\neq x_q} |P_p \cap P_q| + |P_1|n^{3/2+\epsilon}.\end{aligned}$$

We can therefore fix two distinct points $p, q \in P_1$ with $x_p \neq x_q$ such that

$$|P_p \cap P_q| \gg \frac{n^{2-4\epsilon}}{|P|} \gg n^{1-4\epsilon}.$$

Now let $P' = P_p \cap P_q$ and note that

$$I(P', L) = \sum_{p\in P'} \sum_{l\in L} \delta_{pl} \geq |P'|n^{1/2-\epsilon} \gg n^{3/2-5\epsilon}.$$

Since $I(P^{x_p}, L) \leq n$ we can discard all points in P^{x_p} other than p, and thereby assume $P^{x_p} = \{p\}$.

At this point we diverge from [2] and [6]. All we shall carry forward are the facts that:

- $|P'|, |L| \leq n$.
- $I(P', L) \gg n^{3/2-5\epsilon}$.
- P' is a $(2, \lambda)$-strong-antifield.
- There are two points p, q, lying on distinct vertical lines, such that $P' = P_p \cap P_q$ where P_p is a set of points lying on $O(n^{1/2+\epsilon})$ lines through p, and P_q is a set of points lying on $O(n^{1/2+\epsilon})$ lines through q.
- No point in P' lies on the vertical line through p.

These facts are unaffected by translation and so without loss of generality we shall assume that p is in fact the origin.

Recall that the *projective plane* $\mathbb{P}^2(F)$ is defined to be $F^3 \setminus (0, 0, 0)$, modulo dilations. We embed $F \times F$ in $\mathbb{P}^2(F)$ by identifying $(x, y) \in F \times F$ with $(x, y, 1) \in \mathbb{P}^2(F)$. This accounts for all elements of $\mathbb{P}^2(F)$ apart from those of the form $(x, y, 0)$; these are said to lie on the *line at infinity*. For our purposes, the only such point we need consider is $(1, 0, 0)$. Every line incident to this point has gradient 0, and is therefore horizontal. A *projective transformation* is an invertible linear map from $\mathbb{P}^2(F)$ to itself, i.e. a 3×3 non-singular matrix, and has the important property that it maps points to points and lines to lines, thereby preserving the number of incidences.

Returning to the proof, we apply the projective transformation τ given by

$$\tau = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

Note that:

- $I(\tau(P'), \tau(L)) = I(P', L) \gg n^{3/2-5\epsilon}$.
- τ maps the y-axis to the line at infinity. In particular, it maps the origin (which we have assumed to be p) to the point at infinity with gradient 0, and so the points in $\tau(P_p)$ lie on $O(n^{1/2+\epsilon})$ horizontal lines.
- Since P' has no points on the y-axis, the image $\tau(P')$ is contained in $F \times F$.
- Since q does not lie on the y-axis, the point $\tau(q)$ lies in $F \times F$ and not on the line at infinity. Every point in $\tau(P_q)$ lies on one of $O(n^{1/2+\epsilon})$ lines through $\tau(q)$.
- $\tau(x, y) = (1/x, y/x)$ for each point (x, y) with $x \neq 0$. So the map $x \mapsto x^{-1}$ is a cross-ratio-preserving injection from $\{x : (x, y) \in \tau(P')\}$ to $\{x : (x, y) \in P'\}$. Since P' is a $(2, \lambda)$-strong-antifield, Lemma 1 implies that $\tau(P)$ is a $(2, \lambda)$-antifield.

From the above we see that we have a $(2, \lambda)$-antifield $P^* = \tau(P')$ and a line set $L^* = \tau(L)$ such that:

- $|P^*|, |L^*| \le n$.
- $I(P^*, L^*) \gg n^{3/2-5\epsilon}$.
- Each point in P^* lies on
  (a) one of $O(n^{1/2+\epsilon})$ lines in L^* that pass through a single point s in $F \times F$,
  (b) one of $O(n^{1/2+\epsilon})$ horizontal lines in L^*.

The properties above are again invariant under translation and so without loss of generality we may assume that s is the origin. And since each horizontal line in P^* contributes at most n incidences we can discard points to assume that $0 \notin B$. We then take A to be the set of gradients of the $O(n^{1/2+\epsilon})$ lines through the origin, and B to be the y-intercepts of the $O(n^{1/2+\epsilon})$ horizontal lines. This completes the proof of the proposition.

5. Lemmata for proving Proposition 2. This section collects the technical lemmata that will be used to prove Proposition 2.

5.1. Pivoting results. We will make use of some "pivoting" results. The first, Lemma 4, was applied in the Helfgott–Rudnev proof [6], and before that in e.g. [5], [4], [8], [11] and [9]. It is stated here without proof.

Lemma 4 (Pivoting lemma 1). *Let F be a field, let $Z \subseteq F$ and let $R(Z) = \frac{Z-Z}{Z-Z}$. Let $a, b \in F$. Then if $|R(Z)| \geq |Z|^2$ there exist $z_1, z_2, z_3, z_4 \in aZ + b$ such that for all $Z' \subseteq Z$ with $|Z'| \gg |Z|$ we have*

$$|Z|^2 \approx |(z_1 - z_2)Z' + (z_3 - z_4)Z'|.$$

The next lemma is a quick and well-known result that is a necessary tool for the lemma that follows it:

Lemma 5. *Let F be a field, let $Z \subseteq F$ and let $R(Z) = \frac{Z-Z}{Z-Z}$. If $x \notin R(Z)$ then $|Z + xZ| \approx |Z|^2$.*

Proof. Clearly $|Z + xZ| \ll |Z|^2$, so we seek $|Z + xZ| \gg |Z|^2$. If there exist $z_1, z_2, z_3, z_4 \in Z$ with $z_2 \neq z_4$ and $z_1 + xz_2 = z_3 + xz_4$, then we can write $x = (z_1 - z_3)/(z_2 - z_4)$, which contradicts the fact that $x \notin R(Z)$. So there is only one way of writing each $v \in Z + xZ$ in the form $v = z_1 + xz_2$ with $z_1, z_2 \in Z$. We therefore have $|Z + xZ| = |Z|(|Z| - 1)/2 \gg |Z|^2$, as required. ∎

Lemma 6, due to Katz and Shen [7], generalises an approach that is traditionally used in conjunction with Lemma 4. The generalisation means that the result allows for the possibility of non-trivial additive subgroups.

Lemma 6 (Pivoting lemma 2). *Let F be a field and let $Z \subseteq F$ be finite such that $R(Z) = \frac{Z-Z}{Z-Z}$ is not a subfield of F. Let $a, b \in F$. Then either*

1. $R(aZ + b)$ is not closed under multiplication, *in which case there exist $x_1, x_2, z_1, z_2, z_3, z_4 \in Z$ such that*

$$|Z'|^2 \leq |x_1(z_1 - z_2)Z' - x_2(z_1 - z_2)Z' + x_1(z_3 - z_4)Z'|$$

for all $Z' \subseteq Z$, or

2. $R(aZ + b)$ is closed under multiplication but is not closed under addition, *in which case there exist $y_1, y_2, y_3, y_4 \in Z$ such that*

$$|Z'|^2 \leq |(y_1 - y_2)Z' + (y_3 - y_4)Z' + (y_3 - y_4)Z'|$$

for all $Z' \subseteq Z$.

Proof. Note that $R(aZ+b) = R(Z)$ so without loss of generality we may assume $a = 1$ and $b = 0$.

Case 1. Since $R(Z) \cdot R(Z) \neq R(Z)$ there are $x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4 \in Z$ with

$$\frac{x_1 - x_2}{x_3 - x_4} \frac{y_1 - y_2}{y_3 - y_4} \notin R(Z).$$

This can be written as

$$\frac{x_1 - x_2}{x_1} \frac{x_1}{x_1 - x_3} \frac{x_1 - x_3}{x_4} \frac{x_4}{x_3 - x_4} \frac{y_1 - y_2}{y_3 - y_4} \notin R(Z)$$

and so there are $a_1, a_2, b_1, b_2, b_3, b_4 \in Z$ with $\frac{a_1-a_2}{a_1}\frac{b_1-b_2}{b_3-b_4} \notin R(Z)$. Therefore, for any $Z' \subseteq Z$,

$$\begin{aligned}|Z'|^2 &\approx \left|Z' + \frac{a_1-a_2}{a_1}\frac{b_1-b_2}{b_3-b_4}Z'\right| \\ &\le |a_1(b_1-b_2)Z' - a_2(b_1-b_2)Z' + a_1(b_3-b_4)Z'|.\end{aligned}$$

This completes the proof of Case 1.

Case 2. We seek $z_1, z_2, z_3, z_4 \in Z$ such that $\frac{z_1-z_2}{z_3-z_4} + 1 \notin R(Z)$. We will then be done, as for any $Z' \subseteq Z$ we will have

$$\begin{aligned}|Z'|^2 &\approx \left|Z' + \left(\frac{x_1-x_2}{x_3-x_4} + 1\right)Z'\right| \\ &\le |(x_1-x_2)Z' + (x_3-x_4)Z' + (x_3-x_4)Z'|.\end{aligned}$$

Since $R(Z) + R(Z) \neq R(Z)$ there are $x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4 \in Z$ with

$$\frac{x_1-x_2}{x_3-x_4} + \frac{y_1-y_2}{y_3-y_4} \notin R(Z).$$

On the other hand, since $R(Z) \cdot R(Z) = R(Z)$ there are $z_1, z_2, z_3, z_4 \in Z$ with

$$\frac{x_1-x_2}{x_3-x_4}\frac{y_3-y_4}{y_1-y_2} = \frac{z_1-z_2}{z_3-z_4}.$$

Combining these two facts gives

$$\frac{z_1-z_2}{z_3-z_4} + 1 = \frac{x_1-x_2}{x_3-x_4}\frac{y_3-y_4}{y_1-y_2} + 1 = \frac{y_3-y_4}{y_1-y_2}\left(\frac{x_1-x_2}{x_3-x_4} + \frac{y_1-y_2}{y_3-y_4}\right) \notin R(Z).$$

This completes the proof of Case 2 and therefore of the lemma. ∎

We will also use the following lemma, due to Katz and Shen. A proof can be found in [7].

Lemma 7. *If $R(Z) \subseteq G$ for some subfield G of F, then $Z \subseteq aG + b$ for some $a, b \in F$.*

5.2. A lemma about sumsets. The following lemma was used in the Helfgott–Rudnev paper [6], and is originally due to Bourgain [1]:

Lemma 8. *Let F be a field. Let X and Y be finite subsets of F and let $K = \max_{y\in Y}|X + yX|$. Then there exist $x_1, x_2, x_3 \in X$ such that*

$$|(X - x_1) \cap (x_2 - x_3)Y| \gg |Y|\,|X|/K.$$

Proof. Let E be the number of solutions to the equation $x_1 + yx_2 = x_3 + yx_4$ with $x_1, x_2, x_3, x_4 \in X$ and $y \in Y$. Then

$$E = \sum_{y\in Y}\sum_{k\in X+yX}\left|X\cap\left(\frac{X-k}{y}\right)\right|^2 \geq \sum_{y\in Y}\frac{\left(\sum_{k\in X+yX}\left|X\cap\left(\frac{X-k}{y}\right)\right|\right)^2}{|X+yX|}$$
$$\geq \frac{|X|^4|Y|}{K}.$$

So there exist $z_1, z_2 \in X$ for which the equation $x_1 + yz_1 = z_2 + yx_2$ has $\gg |X|^2|Y|/K$ solutions $(x_1, x_2, y) \in X \times X \times Y$. In other words, if $X_1 = X - z_1$ and $X_2 = X - z_2$ then there are $\gg |X|^2|Y|/K$ solutions $(u, v, y) \in X_1 \times X_2 \times Y$ to the equation $v = yu$. By averaging, there is an element $u_* = x_* - z_1 \in X_1$ with $x_* \in X$ such that $v = yu_*$ has $\gg |Y|\,|X|/K$ solutions. Thus

$$|(X - z_2) \cap (x_* - z_1)Y| = |X_2 \cap u_*Y| \gg |Y|\,|X|/K. \blacksquare$$

5.3. Standard results from additive combinatorics. We record some standard results from additive combinatorics. The first formalises a common technique.

Lemma 9 (Popularity pigeonholing). *Let X be a finite set and let $f : X \to [1, N]$ be a function. Then there is a subset $Y \subseteq X$ with $|Y| \gg \sum_{x\in X} f(x)/N$ such that for any $y \in Y$ we have $f(y) \gg \sum_{x\in X} f(x)/|X|$.*

Proof. Let $Y = \{x \in X : f(x) \geq \alpha\}$ where $\alpha = \sum_{x\in X} f(x)/(2|X|)$. We seek to show that $|Y| \gg \sum_{x\in X} f(x)/N$. We see this as follows:

$$\sum_{x\in X} f(x) = \sum_{x:\, f(x)\geq\alpha} f(x) + \sum_{x:\, f(x)<\alpha} f(x) \leq N|Y| + \alpha|X|.$$

So we have

$$|Y| \geq \frac{\sum_{x\in X} f(x) - \alpha|X|}{N} = \frac{\sum_{x\in X} f(x)}{2N} \gg \frac{\sum_{x\in X} f(x)}{N}. \blacksquare$$

We will use the following form of the Plünnecke–Ruzsa inequality, due to Ruzsa [10]:

Lemma 10 (Plünnecke–Ruzsa inequality). *Let $X, B_1, \dots, B_k \subseteq \mathbb{F}_p$. Then*

$$\Big|\sum_{j=1}^{k} B_j\Big| \ll \frac{\prod_{j=1}^{k}|X + B_j|}{|X|^{k-1}}.$$

The following lemma is a version of the Balog–Szemerédi–Gowers theorem. A proof can be found in [13], but this appears to have a typographical error which leads to a factor of K_1^4, rather than the correct exponent of 5 below. See [3] for a proof yielding the exponent of 5.

Lemma 11 (Balog–Szemerédi–Gowers). *Let X, Y be finite subsets of a field. Suppose that there is a subset $G \subseteq X \times Y$ such that*

$$|G| \geq |X|\,|Y|/K_1 \quad \textit{and} \quad |X +^G Y| \leq K_2|X|^{1/2}|Y|^{1/2}.$$

Then there exist $X' \subseteq X$ *and* $Y' \subseteq Y$ *with*

$$|X'| \gg |X|/K_1, \qquad |Y'| \gg |Y|/K_1$$

such that

$$|X' + Y'| \ll K_1^5 K_2^3 |X|^{1/2}|Y|^{1/2}.$$

A proof of the following "covering" result can be found in [11].

LEMMA 12 (Covering lemma). *Let* G *be a group and* $B, C \subseteq G$ *be finite. Let* $\epsilon \in (0,1)$*. Then the number of translates of* C *required to cover* $(1-\epsilon)|B|$ *elements of* B *is* $O_\epsilon(|B+C|/|C|)$*.*

6. Proof of Proposition 2. This section uses the results of Section 5 to prove Proposition 2.

6.1. Structure of the proof. We shall assume that P is a $(2,\lambda)$-antifield for some λ, and then show that the conclusion of the proposition follows when $\lambda \approx T^{65}/(|A|^{130}|B|^{194})$.

The proof of Proposition 2 uses the following three claims, whose proofs are deferred. We shall first see how they are applied to prove the proposition.

CLAIM 1. *There is a subset* $C \subseteq \mathbb{F}_q$ *with* $|C| \gg T^5/(|A|^{10}|B|^{14})$ *such that for each* $c \in C$ *there is a pair of* $(1,\lambda)$*-antifields* $A_c^1, A_c^2 \subseteq F$ *with*

$$|A_c^1|, |A_c^2| \gg \frac{T}{|A|\,|B|^3}, \tag{6}$$

$$|A_c^1 + cA_c^2| \ll \frac{|A|^{11}|B|^{15}}{T^5}. \tag{7}$$

Moreover, there exists $c_* \in C$ *such that, writing* $A_* = A_{c_*}$*, we have*

$$|A_c^1 \cap A_*^1|, |A_c^2 \cap A_*^2| \gg \frac{T^4}{|A|^7|B|^{12}} \tag{8}$$

for all $c \in C$*.*

CLAIM 2. *The following bounds hold for each* $c \in C$*:*

$$|A_c^1 + A_c^1|, |A_c^2 + A_c^2| \ll \frac{|A|^{23}|B|^{33}}{T^{11}}, \tag{9}$$

$$|c_*A_c^2 + cA_c^2| \ll \frac{|A|^{59}|B|^{87}}{T^{29}}, \tag{10}$$

$$|c_*A_*^2 + cA_c^2| \ll \frac{|A|^{89}|B|^{132}}{T^{44}}, \tag{11}$$

$$|c_*A_*^2 + cA_*^2| \ll \frac{|A|^{119}|B|^{177}}{T^{59}}. \tag{12}$$

CLAIM 3. *There exists an integer* Γ *with*

$$\Gamma \ll \frac{|A|^{48}|B|^{72}}{T^{24}} \tag{13}$$

such that given any $c \in \pm C$, $x \in \mathbb{F}_q$, and $D \subseteq A^2_*$, a constant proportion of $cD + x$ can be covered with Γ translates of A^1_*.

6.2. Proof of Proposition 2, assuming claims. Apply Lemma 8 with $X = A^2_*$, $Y = (1/c_*)C$ and, by inequality (12), $K \ll |A|^{119}|B|^{177}/T^{59}$. This provides $a_1, a_2, a_3 \in A^2_*$ such that

$$\left|(A^2_* - a_1) \cap \frac{a_2 - a_3}{c_*}C\right| \gg \frac{|A^2_*|\,|C|}{K} \gg \frac{T^{65}}{|A|^{130}|B|^{194}}.$$

For convenience, define $Z = (A^2_* - a_1) \cap \frac{a_2-a_3}{c_*}C$, to give the lower bound

$$|Z| \gg \frac{T^{65}}{|A|^{130}|B|^{194}}. \tag{14}$$

We seek an upper bound for $|Z|$ with which to compare (14). There are three possible cases:

1. *$R(Z)$ is not closed under multiplication.* By Lemma 6 there are then $c_1, c_2, d_1, d_2, d_3, d_4 \in C$ such that for every $Z' \subseteq Z$ with $|Z'| \gg |Z|$ we have
$$|Z|^2 \ll |c_1(d_1 - d_2)Z' - c_2(d_1 - d_2)Z' + c_1(d_3 - d_4)Z'|.$$
2. *$R(Z)$ is closed under multiplication but is not closed under addition.* By Lemma 6 there are then $c_1, c_2, c_3, z_4 \in C$ such that for every $Z' \subseteq Z$ with $|Z'| \gg |Z|$ we have
$$|Z|^2 \ll |(c_1 - c_2)Z' + (c_1 - c_2)Z' + (c_3 - c_4)Z'|.$$
3. *$R(Z)$ is a field*, G say. Lemma 7 implies that in this case $Z \subseteq aG + b$ for some $a, b \in F$. So, collecting together various facts, we have:
   - $Z \subseteq A^2_* - a_1$.
   - A^2_* is a $(1, \lambda)$-antifield, and therefore so is $A^2_* - a_1$.
   - $Z \subseteq aG + b$ for some $a, b \in F$.
   - $|Z| \gg T^{65}/(|A|^{130}|B|^{194})$.

So for some $\lambda \approx T^{65}/(|A|^{130}|B|^{194})$, the definition of a $(2, \lambda)$-antifield implies that $|Z| \leq |G|^{1/2} = |R(Z)|^{1/2}$. Lemma 4 then implies that there are $c_1, c_2, c_3, c_4 \in C$ such that for every $Z' \subseteq Z$ with $|Z'| \gg |Z|$ we have

$$|Z|^2 \ll |(c_1 - c_2)Z' + (c_3 - c_4)Z'|.$$

6.2.1. *Dealing with Case 1.* Given any $Z' \subseteq Z$ with $|Z'| \gg |Z|$ and any $E \subseteq A^2_*$ with $|E| \gg |A^2_*|$, apply Lemma 10 with $X = c_1(d_1 - d_2)E$ and $k = 3$ to get

$$\begin{aligned} |Z|^2 &\ll |c_1(d_1 - d_2)Z' - c_2(d_1 - d_2)Z' + c_1(d_3 - d_4)Z'| \\ &\ll \frac{|E + Z'|\,|c_1E - c_2Z'|\,|d_1E - d_2E + d_3Z' - d_4Z'|}{|A^2_*|^2}. \end{aligned}$$

By definition of Γ from Claim 3, there is a subset $S_1 \subseteq A_*^2$ with $|S_1| \gg |A_*^2|$ such that $d_1 S_1$ can be covered with Γ copies of A_*^1. Further, there is a subset $S_2 \subseteq S_1$ with $|S_2| \gg |S_1| \gg |A_*^2|$ such that $-d_2 S_2$ can be covered with Γ copies of A_*^1. And there is a subset $S_3 \subseteq S_2$ with $|S_3| \gg |A_*^2|$ such that $c_1 S_3$ can be covered with Γ copies of A_*^1. Set $E = S_3$, so that $d_1 E$, $-d_2 E$ and $c_1 E$ can be covered with Γ copies of A_*^1 each.

Similarly, recall that $Z \subseteq A_*^2 - a_1$, and pick $Z' \subseteq Z$ with $|Z'| \gg |Z|$ such that $d_3 Z'$,$-d_4 Z'$ and $-c_2 Z'$ can each be covered with Γ copies of A_*^1. Altogether, this means that

$$\begin{aligned}|Z|^2 &\ll \frac{\Gamma^6 |E + Z'|\,|A_*^1 + A_*^1|\,|A_*^1 + A_*^1 + A_*^1 + A_*^1|}{|A_*^2|^2}\\ &\le \frac{\Gamma^6 |A_*^2 + A_*^2|\,|A_*^1 + A_*^1|\,|A_*^1 + A_*^1 + A_*^1 + A_*^1|}{|A_*^2|^2}.\end{aligned}$$

Lemma 10 and the bound in Claim 3 then give

$$|Z|^2 \ll \frac{\Gamma^6 |A_*^2 + A_*^2|\,|A_*^1 + A_*^1|\,|A_*^1 + c_* A_*^2|^4}{|A_*^2|^5} \ll \frac{|A|^{383}|B|^{573}}{T^{191}}.$$

Comparing with (14) gives $T \ll |A|^{643/321}|B|^{961/321}$, which satisfies the bound in the statement of the proposition.

6.2.2. *Dealing with Case 2.* Given any $Z' \subseteq Z$ with $|Z'| \gg |Z|$ and any $E \subseteq A_*^2$ with $|E| \gg |A_*^2|$ we can apply Lemma 10 with $X = (c_1 - c_2)E$ and $k = 2$ to get

$$\begin{aligned}|Z|^2 &\ll |(c_1 - c_2)Z' + (c_1 - c_2)Z' + (c_3 - c_4)Z'|\\ &\ll \frac{|E + Z' + Z'|\,|c_1 E - c_2 E + c_3 Z' - c_4 Z'|}{|A_*^2|}\\ &\le \frac{|A_*^2 + A_*^2 + A_*^2|\,|c_1 E - c_2 E + c_3 Z' - c_4 Z'|}{|A_*^2|}.\end{aligned}$$

As in Case 1, pick Z' and E so that

$$|Z|^2 \ll \frac{\Gamma^4 |A_*^2 + A_*^2 + A_*^2|\,|A_*^1 + A_*^1 + A_*^1 + A_*^1|}{|A_*^2|}.$$

Lemma 10 then gives

$$|Z|^2 \ll \frac{\Gamma^4 |A_*^1 + c_* A_*^2|^7}{|A_*^1|^2 |A_*^2|^4} \ll \frac{|A|^{275}|B|^{411}}{T^{137}}.$$

Comparing with (14) gives $T \ll |A|^{535/267}|B|^{799/267}$, which satisfies the bound in the statement of the proposition.

6.2.3. *Dealing with Case 3.* As with Cases 1 and 2, pick Z' so that

$$|Z|^2 \ll |(c_1 - c_2)Z' + (c_3 - c_4)Z'| \le \Gamma^4 |A_*^1 + A_*^1 + A_*^1 + A_*^1|.$$

Then Lemma 10 gives

$$|Z|^2 \ll \frac{\Gamma^4 |A_*^1 + c_* A_*^2|^4}{|A_*^2|^3} \ll \frac{|A|^{239}|B|^{357}}{T^{119}}.$$

Comparing with (14) gives $T \ll |A|^{499/249}|B|^{745/249}$, which satisfies the bound in the statement of the proposition.

The proof of the proposition is therefore complete, subject to the proofs of Claims 1, 2 and 3, which are given below.

6.3. Proof of Claim 1. Every point in P is the intersection of a horizontal line in L_B (with y-coordinate lying in B) and a line through the origin in L_A (with gradient lying in A). Denote the lines in L_B by h_b for each $b \in B$ and the lines in L_A by d_a for each $a \in A$. Furthermore, for each $b \in B$ define

$$X_b = \{x \in F : (x, b) \in h_b \cap P\}.$$

Note that X_b is a $(1, \lambda)$-antifield for each $b \in B$ as it is contained in the $(1, \lambda)$-antifield $\{x : (x, y) \in P\}$.

Now, the set $L(P)$ of lines and the set P of points generate T collinear triples. So, by averaging, there are distinct $b_1, b_2 \in B$ such that there are at least $T/|B|^2$ collinear triples $(p_1, p_2, p_3) \in P \times P \times P$ with $p_1 \in h_{b_1}$ and $p_2 \in h_{b_2}$.

By Lemma 9 there is then a set $B' \subseteq B$ with $|B'| \gg T/(|A|^2|B|^2)$ such that, for each $b \in B'$, there are $\gg T/|B|^3$ collinear triples $(p_1, p_2, p_3) \in P \times P \times P$ with $p_1 \in h_{b_1}$, $p_2 \in h_{b_2}$ and $p_3 \in h_b$.

This is the same as saying that for each $b \in B'$ there are $\gg T/|B|^3$ pairs $x_1 \in X_{b_1}$, $x_2 \in X_{b_2}$ for which

$$x_1\left(1 - \frac{b - b_1}{b_2 - b_1}\right) + x_2\left(\frac{b - b_1}{b_2 - b_1}\right) \in X_b.$$

So for each $b \in B'$, we can apply the Balog–Szemerédi–Gowers theorem (Lemma 11) with

$$X = \left(1 - \frac{b - b_1}{b_2 - b_1}\right) X_{b_1},$$

$$Y = \frac{b - b_1}{b_2 - b_1} X_{b_2},$$

$$G = \left\{(x_1, x_2) \in X_{b_1} \times X_{b_2} : x_1\left(1 - \frac{b - b_1}{b_2 - b_1}\right) + x_2 \frac{b - b_1}{b_2 - b_1} \in X_b\right\},$$

$$|G| \gg \frac{T}{|B|^3},$$

$$K_1 = |X_{b_1}|\,|X_{b_2}|\frac{|B|^3}{T},$$
$$K_2 = \frac{|X_b|}{|X_{b_1}|^{1/2}|X_{b_2}|^{1/2}},$$

to find subsets $A_b^1 \subseteq X_{b_1}$ and $A_b^2 \subseteq X_{b_2}$ with

$$\begin{aligned}\left|A_b^1 + \left(\frac{b_1-b_2}{b_2-b} - 1\right)A_b^2\right| &= \left|\left(1 - \frac{b-b_1}{b_2-b_1}\right)A_b^1 + \frac{b-b_1}{b_2-b_1}A_b^2\right| \\ &\ll \frac{|X_b|^3|X_{b_1}|^4|X_{b_2}|^4|B|^{15}}{T^5} \\ &\ll \frac{|A|^{11}|B|^{15}}{T^5},\end{aligned}$$
$$|A_b^1| \gg \frac{T}{|X_{b_2}|\,|B|^3} \gg \frac{T}{|A|\,|B|^3},$$
$$|A_b^2| \gg \frac{T}{|X_{b_1}|\,|B|^3} \gg \frac{T}{|A|\,|B|^3}.$$

Moreover, note that A_b^1 and A_b^2 are both $(1,\lambda)$-antifields for each $b \in B'$ as they are contained in the $(1,\lambda)$-antifields X_{b_1} and X_{b_2} respectively.

By dropping at most one element we may assume that $b_2 \notin B'$. Now let $C' = \left\{\frac{b_1-b_2}{b_2-b} - 1 : b \in B'\right\}$ and note that the map $b \mapsto \frac{b_1-b_2}{b_2-b} - 1$ is a bijection. Define sets A_c^1, A_c^2 by $A_c^i = A_{b(c)}^i$ for each $c \in C'$. Then we have

$$|C'| = |B'| \gg \frac{T}{|A|^2|B|^2},$$
$$|A_c^1 + cA_c^2| \ll \frac{|A|^{11}|B|^{15}}{T^5} \qquad \text{for each } c \in C',$$
$$|A_c^1|, |A_c^2| \gg \frac{T}{|A|\,|B|^3} \qquad \text{for each } c \in C'.$$

Let $P_c = A_c^1 \times A_c^2$, so that $|P_c| \gg T^2/(|A|^2|B|^6)$ for each $c \in C'$. Cauchy–Schwarz implies that

$$|C'|\frac{T^2}{|A|^2|B|^6} \ll \sum_{c\in C'} |P_c| \le |A|\sqrt{\sum_{c,c'\in C'} |P_c \cap P_{c'}|}.$$

So there is a $c^* \in C'$ such that

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

Lemma 9 then yields a subset $C \subseteq C'$ such that

$$|P_c \cap P_{c^*}| \gg \frac{T^4}{|A|^6|B|^{12}} \quad \text{for all } c \in C, \quad |C| \gg \frac{T^5}{|A|^{10}|B|^{14}}.$$

Note that $|P_c \cap P_{c^*}| = |A_c^1 \cap A_{c^*}^1|\,|A_c^2 \cap A_{c^*}^2|$ to see that

$$|A_c^1 \cap A_{c^*}^1|, |A_c^2 \cap A_{c^*}^2| \gg \frac{T^4}{|A|^7|B|^{12}}$$

for each $c \in C$. This completes the proof of the claim.

6.4. Proof of Claim 2. The claim is proved by repeated application of Lemma 10 and inequalities (6)–(8):

6.4.1. *Proof of* (9). Lemma 10 and the inequalities (6) and (7) imply that

$$|A_c^1 + A_c^1| \le \frac{|A_c^1 + cA_c^2|^2}{|A_c^2|} \ll \frac{|A|^{23}|B|^{33}}{T^{11}}.$$

Similarly for $|A_c^2 + A_c^2|$, which completes the proof of (9).

6.4.2. *Proof of* (10). Lemma 10, and inequalities (8) and (9), imply that

$$\begin{aligned}|c_*A_c^2 + cA_c^2| &\le \frac{|c_*A_c^2 + c_*(A_c^2 \cap A_*^2)|\,|cA_c^2 + c_*(A_c^2 \cap A_*^2)|}{|A_c^2 \cap A_*^2|} \\ &\ll \frac{|A_c^2 + A_c^2|}{|A_c^2 \cap A_*^2|}|cA_c^2 + c_*(A_c^2 \cap A_*^2)| \\ &\ll \frac{|A|^{30}|B|^{45}}{T^{15}}|cA_c^2 + c_*(A_c^2 \cap A_*^2)|.\end{aligned}$$

Now apply Lemma 10 again, with (7) and (8), to see that

$$\begin{aligned}|cA_c^2 + c_*(A_c^2 \cap A_*^2)| &\ll \frac{|(A_c^1 \cap A_*^1) + cA_c^2|\,|c_*(A_c^2 \cap A_*^2) + (A_c^1 \cap A_*^1)|}{|A_c^1 \cap A_*^1|} \\ &\le \frac{|A_c^1 + cA_c^2|\,|A_*^1 + c_*A_*^2|}{|A_c^1 \cap A_*^1|} \ll \frac{|A|^{29}|B|^{42}}{T^{14}},\end{aligned}$$

which completes the proof of (10).

6.4.3. *Proof of* (11). Lemma 10, and inequalities (7)–(10), imply that

$$\begin{aligned}|c_*A_*^2 + cA_c^2| &\le \frac{|c_*A_*^2 + c_*(A_c^2 \cap A_*^2)|\,|cA_c^2 + c_*(A_c^2 \cap A_*^2)|}{|A_c^2 \cap A_*^2|} \\ &\le \frac{|A_*^2 + A_*^2|\,|c_*A_c^2 + cA_c^2|}{|A_c^2 \cap A_*^2|} \ll \frac{|A|^{89}|B|^{132}}{T^{44}},\end{aligned}$$

which completes the proof of (11).

6.4.4. *Proof of* (12). Lemma 10, and inequalities (7)–(9) and (11), imply that

$$|c_*A_*^2 + cA_*^2| \ll \frac{|c_*A_*^2 + c(A_c^2 \cap A_*^2)|\,|cA_*^2 + c(A_c^2 \cap A_*^2)|}{|A_c^2 \cap A_*^2|}$$
$$\leq \frac{|c_*A_*^2 + cA_c^2|\,|A_*^2 + A_*^2|}{|A_c^2 \cap A_*^2|} \ll \frac{|A|^{119}|B|^{177}}{T^{59}}.$$

This completes the proof of (12), and therefore of the whole claim.

6.5. Proof of Claim 3. Given $D \subseteq A_*^2$, $x \in \mathbb{F}_q$ and $c \in C$, use the covering lemma (Lemma 12) to cover a constant proportion of $cD + x$ with

$$\frac{|cD + (A_c^1 \cap A_*^1)|}{|A_c^1 \cap A_*^1|} \leq \frac{|cA_*^2 + (A_c^1 \cap A_*^1)|}{|A_c^1 \cap A_*^1|}$$

translates of $A_c^1 \cap A_*^1$, and hence with the same number of translates of A_*^1. Lemma 10 and inequalities (7)–(9) then give

$$\frac{|cA_*^2 + (A_c^1 \cap A_*^1)|}{|A_c^1 \cap A_*^1|} \ll \frac{|cA_*^2 + c(A_c^2 \cap A_*^2)|\,|(A_c^1 \cap A_*^1) + c(A_c^2 \cap A_*^2)|}{|A_c^1 \cap A_*^1|\,|A_c^2 \cap A_*^2|}$$
$$\leq \frac{|A_*^2 + A_*^2|\,|A_c^1 + cA_c^2|}{|A_c^1 \cap A_*^1|\,|A_c^2 \cap A_*^2|} \ll \frac{|A|^{48}|B|^{72}}{T^{24}}.$$

The proof is similar when $c \in -C$. This completes the proof of the claim.

Acknowledgements. The author is grateful to the referee for some helpful comments and corrections, to Oliver Roche-Newton and Misha Rudnev for useful discussions and for pointing out various typographical errors in earlier drafts, and to Nick Gill for asking some awkward questions.

References

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

[2] J. Bourgain, N. Katz, and T. Tao, *A sum-product estimate in finite fields and applications*, ibid. 14 (2004), 27–57.

[3] J. Fox and B. Sudakov, *Dependent random choice*, arXiv:math/0909.3271, 2009.

[4] M. Z. Garaev, *An explicit sum-product estimate in* $\mathbb{F}_p$, Int. Math. Res. Notices 2007, no. 11, 1–11.

[5] A. A. Glibichuk and S. V. Konyagin, *Additive properties of product sets in fields of prime order*, in: Additive Combinatorics, CRM Proc. Lecture Notes 43, Amer. Math. Soc., 2007, 279–286.

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

[7] N. Katz and C.-Y. Shen, *Garaev's inequality in finite fields not of prime order*, Online J. Anal. Combin. 2008, no. 3.

[8] —, —, *A slight improvement to Garaev's sum product estimate*, Proc. Amer. Math. Soc. 136 (2008), 2499–2504.

[9] L. Li, *Slightly improved sum-product estimates in fields of prime order*, arXiv:math/0907.2051, 2009.
[10] I. Z. Ruzsa, *An application of graph theory to additive number theory*, Sci. Ser. A Math. Sci. (N.S.) 3 (1989), 97–109.
[11] C.-Y. Shen, *Quantitative sum product estimates on different sets*, Electron. J. Combin. 15 (2008), no. 1, 7 pp.
[12] E. Szemerédi and W. T. Trotter Jr., *Extremal problems in discrete geometry*, Combinatorica 3 (1983), 381–392.
[13] T. Tao and V. Vu, *Additive Combinatorics*, Cambridge Univ. Press, 2006.
[14] C. Tóth, *The Szemerédi–Trotter theorem in the complex plane*, arXiv:math/0305283v3, 2005.
[15] L. Vinh, *Szemerédi–Trotter type theorem and sum-product estimate in finite fields*, arXiv:math/0711.4427v1, 2007.

Timothy G. F. Jones
School of Mathematics
University of Bristol
Bristol BS8 1TW, United Kingdom
E-mail: tgf.jones@bristol.ac.uk

Received on 25.10.2010
and in revised form on 8.2.2011 (6530)