

UPPER AND LOWER BOUNDS FOR RICH LINES IN GRIDS

BRENDAN MURPHY

ABSTRACT. We prove upper and lower bounds for the number of lines in general position that are rich in a Cartesian product point set. This disproves a conjecture of Solymosi and improves work of Elekes, Borestein and Croot, and Amirkhanyan, Bush, Croot, and Pryby.

The upper bounds are based on a version of the asymmetric Balog-Szemerédi-Gowers theorem for *group actions* combined with product theorems for the affine group. The lower bounds are based on a connection between rich lines in Cartesian product sets and *amenability* (or expanding families of graphs in the finite field case).

As an application of our upper bounds for rich lines in grids, we give a geometric proof of the asymmetric sum-product estimates of Bourgain and Shkredov.

CONTENTS

1. Introduction	1
2. Lower bounds for rich lines in grids	7
3. Upper bounds for rich lines in grids	13
Appendix A. Proof of group action Balog-Szemerédi-Gowers	20
Appendix B. Product theorems for $\text{Aff}(1, \mathbb{F})$	23
References	27

1. INTRODUCTION

Let \mathbb{F} be a field and let $0 < \alpha \leq 1$ be a real number.

A line ℓ in the plane \mathbb{F}^2 is α -*rich* in a Cartesian product point set $Y \times Y \subseteq \mathbb{F}^2$ if

$$|\ell \cap (Y \times Y)| \geq \alpha|Y|.$$

For short, we call $Y \times Y$ a *grid*. Any line contains at most N points of a $N \times N$ grid, so a line is α -rich if it contains α -percent of the maximum possible points of incidence. The parameter α may be a constant independent of N , or may be some small power of $1/N$.

There are two questions we wish to answer about rich lines in grids:

- (1) how many α -rich lines can a $N \times N$ grid support?
- (2) if a grid supports many rich lines, must these lines have some *structure*?

The first question was answered for $\mathbb{F} = \mathbb{R}$ by Szemerédi-Trotter [35]: a $N \times N$ grid has at most $O(\alpha^{-3}N)$ α -rich lines; this is sharp. Below, we discuss extensions of

this upper bound and the examples that provide lower bounds. (We use standard asymptotic notation; see Section 1.4 for definitions.)

The second question is an *inverse problem* for point-line incidences. The inverse problem for the Szemerédi-Trotter theorem is to show that if n points and n lines in \mathbb{R}^2 have $\Omega(n^{4/3})$ incidences, then the point set has some *structure* [9, Problem 5.7]; sharpness examples suggest that the point set might contain a large Cartesian product of arithmetic progressions. Even under the assumption that the point set is a Cartesian product, little is known about the inverse problem for Szemerédi-Trotter. Question 2 has the further simplifying assumption that the lines are *rich*; in this case, it is possible to give a precise description of the set of lines and the point set [12, 13].

Solymosi conjectured that in the *absence* of structure, a grid can support at most a *constant* number of α -rich lines [13, Conjecture 3.10]. A generic collection of lines contains no two parallel lines and no three lines through a common point; such a set of lines is said to be in *general position*. Solymosi's conjecture is the following.

Conjecture 1 ([13, Conjecture 3.10]). Among the lines that are α -rich in a $N \times N$ Cartesian product, at most $C = C(\alpha) > 0$ can be in general position.

In [13], Conjecture 1 is stated for lines defined over \mathbb{R} or \mathbb{C} . Solymosi's conjecture is supported by the sharpness examples for the Szemerédi-Trotter incidence bound, and also implies a plausible conjecture of Elekes [13, Problem 3.9]; see the appendix of [1] for a discussion.

Despite this evidence, Conjecture 1 is false: we disprove it with explicit examples over \mathbb{Q} , \mathbb{C} , and \mathbb{F}_p , the finite field with prime cardinality p . The examples we give are quite different from Cartesian products of arithmetic (or geometric) progressions, which show that the Szemerédi-Trotter incidence bound is sharp and motivate the sum-product conjecture.

Let $RLGP(\mathbb{F}, N, \alpha)$ denote the maximum over all $Y \subseteq \mathbb{F}$ with $|Y| = N$ of the maximum number of lines that are α -rich in $Y \times Y$ and in general position. Explicitly, if $RLGP(A, \alpha)$ is the maximum number of α -rich lines in $A \times A$ that are in general position, then

$$RLGP(\mathbb{F}, N, \alpha) := \max_{A \subseteq \mathbb{F}, |A|=N} RLGP(A, \alpha).$$

Conjecture 1 posits that for $\mathbb{F} = \mathbb{R}$ (or $\mathbb{F} = \mathbb{C}$) and for all $0 < \alpha < 1$, there is a constant $C(\alpha) > 0$ depending on α such that

$$RLGP(\mathbb{F}, N, \alpha) \leq C(\alpha).$$

For $\mathbb{F} = \mathbb{Q}$, we prove a lower bound for $RLGP(\mathbb{Q}, N, \alpha)$ that is nearly logarithmic in N . In particular, this disproves Conjecture 1 for $\mathbb{F} = \mathbb{R}$ and $\mathbb{F} = \mathbb{C}$.

Theorem 2. *There is an absolute constant $C > 0$ such that for any $0 < \alpha < 1$*

$$RLGP(\mathbb{Q}, N, \alpha) \geq C(1 - \alpha) \frac{\log N}{\log \log N}.$$

For $\mathbb{F} = \mathbb{C}$ and $\mathbb{F} = \mathbb{F}_p$, we prove upper and lower bounds for $RLGP(\mathbb{F}, N, \alpha)$ whose logarithms differ by a square root.

Theorem 3. *Let \mathbb{F} denote \mathbb{C} or \mathbb{F}_p . For every $0 < \alpha < 1$, there is a constant $C_\alpha > 0$ such that*

$$\frac{1}{C_\alpha} \sqrt{\frac{\log N}{\log \log N}} \leq \log RLGP(\mathbb{F}, N, \alpha) \leq C_\alpha \frac{\log N}{\log \log N}.$$

If $\mathbb{F} = \mathbb{F}_p$, the upper bound holds only if $N^{1+\log(2/\alpha)/\log \log N} \leq p$.

The upper bound applies when $\mathbb{F} = \mathbb{R}$, since we may consider points and lines defined over \mathbb{R} to be contained in \mathbb{C}^2 .

The upper bound in Theorem 3 is a special case of the following general structure theorem for rich lines in grids over \mathbb{C} and \mathbb{F}_p .

Theorem 4. *There is an absolute constant $C > 0$ such that the following holds. Let Y be a finite subset of \mathbb{F} and let L be a set of α -rich lines in $Y \times Y$. Let $J > 0$ be an integer such that $(\alpha/2)^{2^J} \geq 1/|Y|$.*

If $\mathbb{F} = \mathbb{C}$, then there is a subset $L' \subseteq L$ such that

- (1) the lines of L' are either parallel or concurrent, and*
- (2) $|L'| \gg (\frac{\alpha}{2})^{C \cdot 2^J} |Y|^{-C/J} |L|$.*

If $\mathbb{F} = \mathbb{F}_p$, then the same conclusion holds, provided that $|Y| \leq (\alpha/2)^{2^J} p$.

The key point is that by taking J sufficiently large, the factor $|Y|^{-C/J}$ becomes negligible. Theorem 4 is a consequence of a version of the asymmetric Balog-Szemerédi-Gowers theorem for *group actions*, proved in [26], combined with a *product theorem* for the affine group.

The lower bounds in Theorems 2 and 3 follow from explicit constructions; see Theorems 10, 11, and 15 in Section 2. If Conjecture 1 were true over \mathbb{R} , then subgroups of $\text{Aff}(1, \mathbb{R})$ generated by a finite set of affine transformations in general position would not be *amenable*, however finitely generated solvable groups are amenable; Theorem 10 proves this quantitatively. Heuristically, if Conjecture 1 were true over \mathbb{F}_p , it might be possible to make an expanding family of Schreier graphs for $\text{Aff}(1, \mathbb{F}_p) \curvearrowright \mathbb{F}_p$ with bounded degree (following a similar strategy to Bourgain and Gamburd [4]), however this is known to be false by a theorem of Lubotzky and Weiss [24, 25]. To prove the lower bound in Theorem 3, we use a construction of Klawe [22, 23], which gives a quantitative proof of Lubotzky and Weiss' theorem for $\text{Aff}(1, \mathbb{F}_p) \curvearrowright \mathbb{F}_p$; using a theorem of Grosu [18], we embed our counter-example into \mathbb{C}^2 .

In Section 2 we construct examples of grids that support many α -rich lines, and in Section 3 we prove upper bounds the number of α -rich lines supported by a $N \times N$ grid. These sections are completely independent. The remainder of the introduction contains background on rich lines in grids and some positive results towards Conjecture 1, as well as an explanation of the connection between rich lines and grids and sum-product problems.

For completeness, we sketch the proof of the group action version of the Balog-Szemerédi-Gowers theorem and prove the necessary product theorems for affine transformations in Appendices A and B. In particular, Appendix A gives a proof of Elekes' Theorem 5 and compares it with the proof of Theorem 4.

1.1. Background on rich lines in grids. As mentioned, the Szemerédi-Trotter theorem [35] implies that $O(\alpha^{-3}N)$ lines may be α -rich in a $N \times N$ grid in \mathbb{R}^2 . This lower bound is attained by two simple examples, up to factors of α .

- (1) If $Y = \{1, \dots, N\}$, then the parallel lines $\ell(x) = x + b$ are α -rich for $b \ll (1 - \alpha)N$, thus $Y \times Y$ supports roughly N parallel α -rich lines.
- (2) If $Y = \{1, 2, \dots, 2^{N-1}\}$, then the lines $\ell(x) = 2^j x$ through the origin are α -rich for $j \ll (1 - \alpha)N$, thus $Y \times Y$ supports roughly N concurrent α -rich lines.

A more elaborate example, due to Erdős, achieves the correct power of α .

Example. Let N be a large positive integer, let $Y = \{n \in \mathbb{Z}: |n| \leq N\}$ and let $P = Y \times Y$. For coprime integers $a < b$, define a set of lines

$$L_{a,b} = \{y - j = \frac{a}{b}(x - i): 1 \leq i \leq b, 1 \leq j \leq \frac{N}{2}\}.$$

Each line in $L_{a,b}$ is incident to at least $\frac{N}{2b} - 1$ points of P , and thus is α -rich in P for $b \leq \lfloor \frac{1}{3\alpha} \rfloor$. On the other hand, the number of such lines is $\Theta(\alpha^{-3}N)$. See [31] for details.

The following theorem of Elekes [10, 13] says that combinations of examples (1) and (2) are essentially the only possibilities.

Theorem 5 (Elekes). *Let $0 < \alpha \leq 1$ be a constant. If N lines are α -rich in an $N \times N$ grid in \mathbb{R}^2 , then either*

- (1) $C\alpha^C N$ lines are parallel, or
- (2) $C\alpha^C N$ lines are concurrent (incident to a common point),

where $C > 0$ is a constant independent of α and N .

By applying Freiman's theorem, Elekes concludes that the family of parallel lines obtained in Theorem 5 have y -intercepts in a generalized arithmetic progression (similarly, if the lines are concurrent, then their slopes are in a generalized geometric progression) [12, 13].

Elekes reduces the proof of Theorem 5 to a *product theorem*. If A and B are finite sets of real affine transformations, then we define their *composition set* by

$$A \circ B := \{\ell_a \circ \ell_b: \ell_a \in A, \ell_b \in B\}.$$

The collection of affine transformations is a group with product given by composition of functions, so $A \circ B$ is just the product set of A and B .

Theorem 6 (Elekes [10, Theorem 1]). *For every $K > 0$ there is a constant $\rho = \rho(K) > 0$ depending on K with the following property.*

Suppose A, B are finite sets of real affine transformations with $|A|, |B| \geq N$ and

$$|A \circ B| \leq KN$$

Then there exist subsets $A' \subseteq A$ and $B' \subseteq B$ with $|A'|, |B'| \geq \rho N$ such that either

- (1) *both A' and B' consist of parallel lines, or*
- (2) *both A' and B' consist of concurrent lines.*

Though it is not explicit in Elekes' work, ρ depends polynomially on K . Parallel and concurrent lines correspond to cosets of abelian subgroups of the affine group, thus Theorem 6 perhaps the first instance of a product theorem for a non-commutative group. Such theorems have now been studied extensively [5, 7, 8, 16, 19, 20, 29].

The assumption that $|L| \approx |Y|$ is essential for Elekes' reduction of Theorem 5 to Theorem 6. Borenstein and Croot [2] made the first step towards removing this

restriction. Building on [2], Amirkhanyan, Bush, Croot, and Pryby [1] proved an analog of Conjecture 1 where $\alpha = N^{-\delta}$ for some small $\delta > 0$.

Theorem 7 (Amirkhanyan, Bush, Croot, and Pryby). *For all $\varepsilon > 0$ there exists a $\delta > 0$ such that the following holds for all sufficiently large positive integers N :*

If L is a set of N^ε lines in \mathbb{R}^2 that are $\alpha = N^{-\delta}$ -rich in an $N \times N$ grid, then the lines of L are not in general position.

Theorem 7 implies that for all $\varepsilon > 0$, if N is sufficiently large, then

$$RLGP(\mathbb{R}, N, \alpha) \leq N^\varepsilon.$$

In [1, 2], the relationship between ε and δ is not explicit, so it is unclear how strong of a bound this method can achieve.

Borenstein and Croot roughly follow Elekes' method: they reduce to the case of small product set, then contradict structural hypotheses about the initial set of lines. They do not use Theorem 6 (or a similar theorem), but instead use sum-product results, some of which are unique to \mathbb{R} . In particular, it is not clear that their methods should extend to \mathbb{F}_p or to other questions about rich transformations for other groups, such as linear fractional transformations [14].

We use a *group action* version of the Balog-Szemerédi-Gowers theorem [26] to reduce the proof of Theorem 4 to a product theorem for the affine group; in particular, over \mathbb{R} we could use Elekes' Theorem 6. The group action Balog-Szemerédi-Gowers theorem is a generalization of Tao and Vu's asymmetric Balog-Szemerédi-Gowers theorem [37, Theorem 2.35]. Helfgott pointed out that Borenstein and Croot's method is similar to Tao and Vu's method [2]. The group action Balog-Szemerédi-Gowers theorem is a common generalization of these methods.

1.2. Connection to the sum-product problem. Theorem 5 implies a non-trivial *sum-product estimate*. A sum-product estimate is a lower bound of the form

$$|A + A| + |AA| \gg |A|^{1+c}$$

where A is a finite subset of \mathbb{R} (or more generally, a ring), $c > 0$, and $A + A$ and AA are the sets of pairwise sums and pairwise products of elements in A , respectively. Erdős and Szemerédi [15] conjectured that c can be taken arbitrarily close to 1. Elekes [11] gave a beautiful geometric proof of a sum-product estimate with $c = 1/4$, based on the Szemerédi-Trotter bound.

The following sum-product estimate follows from Theorem 5, using the method of [11].

Corollary 8. *Let A, B , and C be finite subsets of \mathbb{R} with $|B||C| = |A|$. There is an absolute constant $c > 0$ such that if $|B|, |C| \geq |A|^\varepsilon$ for some $\varepsilon > 0$, then*

$$|A + B| + |AC| \gg |A|^{1+c\varepsilon}.$$

Proof. Let $\ell_{b,c}(x) = c(x - b)$ and let L denote the set of $\ell_{b,c}$ with $b \in B$ and $c \in C$. Since $|B|, |C| \geq |A|^\varepsilon$, at most $|A|^{1-\varepsilon}$ lines of L are parallel or concurrent.

Set $Y = (A + B) \cup (AC)$. Each line of L is incident to at least $|A|$ points of $Y \times Y$.

If

$$|A + B| + |AC| \leq K|A|,$$

then each line of L is α -rich in $Y \times Y$ with $\alpha = 1/2K$.

By Theorem 5, at least $C_0\alpha^{C_0}|L|$ lines of L are parallel or concurrent, thus we have

$$K^{-C_0}|A| \ll |A|^{1-\varepsilon} \implies K \gg |A|^{\varepsilon/C_0}.$$

By choosing K to be a sufficiently small power of $|A|$, we have a contradiction. \square

The stronger conclusion of Theorem 4 over Theorem 7 allows us to give a geometric proof of Bourgain's asymmetric sum-product estimate [3].

Theorem 9 (Asymmetric sum-product estimate). *Let A, B , and C be finite subsets of a field \mathbb{F} .*

If $\mathbb{F} = \mathbb{C}$ and there is an $\varepsilon > 0$ such that $|B|, |C| \geq |A|^\varepsilon$, then there exists a constant $c = c(\varepsilon) > 0$ such that

$$|A + B| + |AC| \gg |A|^{1+c}.$$

If $\mathbb{F} = \mathbb{F}_p$, the same result holds provided that $|A| \ll p^{1-O(\varepsilon)}$.

In fact, we achieve estimates comparable to those of Shkredov [32]: we may take $c = 1/(J2^J)$ for $J \approx \gamma\varepsilon$. See Theorem 20 for the exact quantitative statement.

1.3. Acknowledgements. I would like to thank the following people for helpful conversations and for reading various drafts of this work: Ernie Croot, Harald Helfgott, Alex Iosevich, John Mackay, Jonathan Pakianathan, Sarah Peluse, Giorgis Petridis, Misha Rudnev, Ilya Shkredov, Jozsef Solymosi, Sophie Stevens, and Yufei Zhao. I would also like to thank the Arizona Winter School and the Simons Institute, whose workshops resulted in several of the key ideas in this work, as well as the Heilbronn Institute for Mathematical Research and the University of Rochester, who funded these trips.

1.4. Notation. We use standard asymptotic notation: $f = O(g)$ means that there is a constant $C > 0$ such that $|f(x)| \leq Cg(x)$ for all x ; $f \ll g$ means the same as $f = O(g)$, $f = \Omega(g)$ and $f \gg g$ mean the same as $g \ll f$. The notation $f \approx g$ means that $f \ll g$ and $g \ll f$; $f = \Theta(g)$ means $f \approx g$. We abuse asymptotic notation slightly for stating hypotheses: a condition of the form $f \ll g$ means that there exists a constant C such that if $|f| \leq Cg$, then the theorem holds. Notation such as $f \ll_\alpha g$ or $f = O_\varepsilon(g)$ means that the implicit constant C depends on the parameter in the subscript.

Unless otherwise stated, we use the following notation throughout:

- α denotes a real number in $(0, 1]$,
- lower case greek letters denote (typically small) real parameters,
- C denotes a positive constant, which may change from line to line,
- \mathbb{F} denotes a field, which may be $\mathbb{R}, \mathbb{C}, \mathbb{Q}$, or \mathbb{F}_p , the finite field with prime cardinality p ,
- Y denotes a finite subset of \mathbb{F} , and N denotes $|Y|$,
- L denotes a finite set of lines in $\mathbb{F}^2 = \mathbb{F} \times \mathbb{F}$,
- G denotes the group $\text{Aff}(1, \mathbb{F})$ of affine transformations of \mathbb{F} ; we represent elements of $\text{Aff}(1, \mathbb{F})$ by linear functions $x \mapsto ax + b$ with $a, b \in \mathbb{F}$, $a \neq 0$, with composition as the group operation,
- A denotes a finite subset of $G = \text{Aff}(1, \mathbb{F})$.

2. LOWER BOUNDS FOR RICH LINES IN GRIDS

In this section, we disprove Conjecture 1, which we recall here.

Conjecture 1. *Among the lines in \mathbb{F}^2 that are α -rich in an $N \times N$ Cartesian product set, at most $C = C(\alpha) > 0$ lines are in general position.*

In terms of symmetry sets, Conjecture 1 states that for any $0 < \alpha < 1$ and any subset $Y \subseteq \mathbb{F}$, at most C transformations in $\text{Sym}_\alpha(Y)$ are in general position.

In Section 2.1, we disprove Conjecture 1 over \mathbb{Q} with an explicit construction. In Section 2.2, we give an explicit construction of a large set of lines in general position in \mathbb{F}_p^2 . In Section 2.3, we embed the counter-examples from the previous section into \mathbb{C}^2 .

2.1. Quantitative lower bounds over \mathbb{R} . In this section, we give an explicit construction of arbitrarily large finite sets Y in \mathbb{R} such that $\text{Sym}_\alpha(Y)$ contains a large number of affine transformations in general position. In fact, the construction only uses rational numbers.

Theorem 10. *For all $0 < \alpha \leq 1$ and all $N_0 > 0$ there exists a set $Y \subseteq \mathbb{Q}$ such that $|Y| \geq N_0$ and $Y \times Y$ supports a set L of α -rich lines in general position such that*

$$|L| \gg (1 - \alpha) \frac{\log |Y|}{\log \log |Y|}.$$

The construction is based on the construction of explicit Følner sequences for $\text{Aff}(1, \mathbb{R})$ acting on \mathbb{R} [17, 40].

Proof of Theorem 10. Fix $0 < \varepsilon < 1$ such that $2\varepsilon \leq 1 - \alpha$. Fix an integer $N > 0$ so that $N^{N+1} \geq N_0$.

Define a subset $Y \subseteq \mathbb{Q}$ of size N^{N+1} by

$$Y := \left\{ N^k \left(N + \sum_{j=0}^{N-1} a_j N^{-j} \right) : 0 \leq k < N, 0 \leq a_j < N \right\}.$$

Since $a_0, \dots, a_{N-1} < N$, we have

$$\sum_{j=0}^{N-1} a_j N^{-j} \leq N \left(1 - \frac{1}{N^N} \right),$$

hence every choice of k and a_0, \dots, a_{N-1} yields a distinct element of Y , and Y has cardinality $N \cdot N^N$, as claimed.

Let L denote the set of transformations defined by $\ell_k(x) := N^k x + k$, where k ranges over integers satisfying $0 < k < \varepsilon N$. We make two claims.

Claim 1. *The transformations in L are in general position.*

Claim 2. *For all ℓ in L , we have*

$$|\ell(Y) \setminus Y| \leq 2\varepsilon |Y|,$$

hence $|\ell \cap (Y \times Y)| \geq \alpha |Y|$ by our choice of ε .

The proof is complete assuming these claims.

To prove Claim 1, it suffices to show that if $0 < i < j < k < \varepsilon N$, then

$$(1) \quad \det \begin{pmatrix} 1 & 1 & 1 \\ N^i & N^j & N^k \\ i & j & k \end{pmatrix} \neq 0.$$

The left-hand side of (1) is

$$(k-i)N^j - (j-i)N^k - (k-j)N^i < (k-i)N^j - (j-i)N^k,$$

which is strictly less than zero:

$$(k-i)N^j < \varepsilon N^{j+1} \leq \varepsilon N^k \leq N^k \leq (j-i)N^k.$$

To prove Claim 2, fix an element ℓ_b in L and consider its action on a general element y of Y :

$$\ell_b(y) = N^{b+k} \left(N + bN^{-(b+k)} + \sum_{j=0}^{N-1} a_j N^{-j} \right).$$

There are two cases where $\ell_b(y) \notin Y$:

- (1) $b+k \geq N$,
- (2) $b+k < N$, but $b+a_{b+k} \geq N$.

At most b values of k satisfy (1), hence at most $bN^N \leq \varepsilon|Y|$ elements of Y fall into the first case. At most b values of a_{b+k} satisfy (2), hence at most $N \cdot bN^{N-1} \leq \varepsilon|Y|$ elements of Y fall into the second case. \square

2.2. Quantitative lower bounds over \mathbb{F}_p . In this section, we prove the lower bound in Theorem 3 for $\mathbb{F} = \mathbb{F}_p$.

Theorem 11. *For any prime p , any $0 < \alpha < 1$, any $\varepsilon > 0$, and any integer m satisfying $1 \ll_\varepsilon m \ll p^{1-\varepsilon}$, there exists a subset $Y \subseteq \mathbb{F}_p$ with $|Y| \approx_\alpha m$ and a set of lines S in general position that are α -rich in $Y \times Y$ such that*

$$\log |S| \approx_\alpha \sqrt{\frac{\log |Y|}{\log \log |Y|}}.$$

The proof of Theorem 11 is based on a construction of Klawe [22, 23], which proves explicitly that Schreier graphs of $\text{Aff}(1, \mathbb{Z}/n\mathbb{Z}) \curvearrowright \mathbb{Z}/n\mathbb{Z}$ cannot be made into an expander family of constant degree. (Lubotzky [25] gives a qualitative proof of this fact using the method of [24].)

Before we state Klawe's theorem, we need some notation. Let $Q = \{q_1, \dots, q_k\}$ denote a set of k primes. We say that n is a Q -power if $n = q_1^{\alpha_1} \cdots q_k^{\alpha_k}$ and in this case, we write $\mu(n) = \alpha_1 + \cdots + \alpha_k$. We use $\phi(n)$ to denote the number of positive integers less than and relatively prime to n .

Theorem 12 (Klawe). *Let $Q = \{q_1, \dots, q_k\}$ be a set of k prime numbers and set $q = q_1 \cdots q_k$. Let N, M, L, r , and s be positive integers such that $N = Mq^s + r$, $0 \leq r < q$, and $L < M/q^s$.*

Then there exists a subset $Y \subseteq \mathbb{Z}/N\mathbb{Z}$ such that

$$(2) \quad |Y| = s^k L \phi(q) q^{s-1}$$

and for all positive integers $0 < a, b < N$ such that a is a Q -power

$$(3) \quad |(aY + b) \setminus Y| \leq \left(\frac{\mu(a)}{s} + \frac{ar+b}{L} \frac{q}{\phi(q)} \right) |Y|.$$

The proof of Theorem 12 uses a construction similar to that of Theorem 10, but uses wrap-around to allow a much larger set of “slopes” a .

We use the following corollary of Theorem 12 to prove Theorem 11.

Corollary 13. *Let $Q = \{q_1, \dots, q_k\}$ be a set of k prime numbers and set $q = q_1 \cdots q_k$. Let p be a prime and let M, L, r , and s be positive integers such that $p = Mq^s + r$, $0 \leq r < q$, and $L < M/q^s$.*

If

$$(4) \quad L \geq \frac{8q}{\phi(q)} \max \left(q^{(1+\frac{1}{4k})s}, \left(\frac{s}{4k} \right)^{2k} \right),$$

then there exists a subset $Y \subseteq \mathbb{F}_p$ satisfying (2) and a set S of affine transformations in general position such that $|S| \geq (s/4k)^k$ and $|\ell(Y) \setminus Y| \leq \frac{1}{2}|Y|$ for all transformations ℓ in S .

Proof. Applying Theorem 12 with $N = p$ yields a set $Y \subseteq \mathbb{F}_p$ such that (2) holds and for all positive integers a and b such that a is a Q -power (3) holds.

We wish to choose a collection of pairs (a, b) such that the corresponding set of lines $\ell(x) = ax + b$ are in general position and satisfy

$$(5) \quad \frac{\mu(a)}{s} + \frac{ar + b}{L} \frac{q}{\phi(q)} \leq \frac{1}{2}.$$

First, we will find a large number of integers a, b satisfying

$$(6) \quad \mu(a) \leq \frac{s}{4}$$

and

$$(7) \quad ar + b \leq \frac{\phi(q)L}{4q}.$$

Let A denote the set of positive integers of the form $a = q_1^{\alpha_1} \cdots q_k^{\alpha_k}$ where $0 \leq \alpha_i \leq s/4k$ for $i = 1, \dots, k$. Then each element a in A satisfies (6) and further $1 \leq a \leq q^{s/4k}$.

If $a \in A$ and b is a positive integer, then

$$ar + b < q^{(1+\frac{1}{4k})s} + b.$$

By (4), we have $\phi(q)L/4q \geq 2q^{(1+\frac{1}{4k})s}$, so (7) is satisfied for all $0 \leq b \leq \phi(q)L/8q$.

Note that $q^{s/4k} < p$ and $\phi(q)L/8q < p$, so a and b are unique modulo p .

To form our set of lines L , we will choose slopes a from A one at a time, choosing y -intercepts $0 \leq b \leq \phi(q)L/8q$ so that the line $\ell(x) = ax + b$ intersects each previous line in a distinct point; this guarantees that no three lines in L are incident to a common point. Since all of the lines in L have distinct slopes, the resulting set of lines L will be in general position.

If we have chosen x lines by this process, then we must avoid $\binom{x}{2}$ points; this is always possible if we have more than $\binom{x}{2}$ choices for b . By (4),

$$\#(\text{choices for } b) \geq \frac{\phi(q)L}{8q} \geq \left(\frac{s}{4k} \right)^{2k} > \binom{x}{2} \quad \text{for all } 0 \leq x \leq |A|.$$

□

We want to take k as large as possible relative to q ; the following lemma gives $k \approx \log q / \log \log q$.

Lemma 14. *Given $x > 0$, let $Q = \{q_1, \dots, q_k\}$ denote the set of primes less than or equal to x , and let $q = q_1 \cdots q_k$. We have the following estimates:*

$$(8) \quad k = |Q| = \frac{x}{\log x} \left(1 + O\left(\frac{1}{\log x}\right) \right),$$

$$(9) \quad q = e^{x(1+O(\frac{1}{\log x}))},$$

and

$$(10) \quad \frac{\phi(q)}{q} = \frac{e^{-\gamma}}{\log x} \left(1 + O\left(\frac{1}{\log x}\right) \right),$$

where γ is Euler's constant.

Proof. Equation (8) is the Prime Number Theorem. Equation (9) follows from asymptotic estimates for Chebyshev's function $\vartheta(x)$:

$$\vartheta(x) = \sum_{p \leq x} \log p = x \left(1 + O\left(\frac{1}{\log x}\right) \right).$$

Equation (10) is Merten's formula [21, Equation (2.16)]. \square

For simplicity, we will prove Theorem 11 for the case $\alpha = \frac{1}{2}$; the general case follows in the same way, with implicit constants depending on α .

Proof of Theorem 11. Let x be a positive real number and let $Q = \{q_1, \dots, q_k\}$ denote the set of primes less than or equal to x . Let $q = q_1 \cdots q_k$ and let $s = \lceil 4e \cdot k \rceil$. For convenience, let $\delta = 1/4k$.

Set

$$L = \frac{8q}{\phi(q)} q^{(1+\delta)s}.$$

Condition (4) of Corollary 13 holds if $q^{(1+\delta)s} \geq (s/4k)^{2k}$. By Lemma 14,

$$q^{(1+\delta)s} \geq q^{4k} = e^{2k \cdot 2x(1+O(\frac{1}{\log x}))},$$

while

$$\left(\frac{s}{4k}\right)^{2k} \leq \left(e + \frac{1}{4k}\right)^{2k} \ll e^{2k},$$

thus condition (4) holds if $x \gg 1$.

Write $p = Mq^s + r$, where $0 \leq r < q^s$ and $M > q^s L$. By Corollary 13 there is a set $Y \subseteq \mathbb{F}_p$ such that

$$(11) \quad |Y| = s^k L \phi(q) q^{s-1} = 8s^k q^{(2+\delta)s}$$

and a set S of lines in general position that are $\frac{1}{2}$ -rich in $Y \times Y$ such that

$$(12) \quad |S| \geq \left(\frac{s}{4k}\right)^k \geq e^k.$$

By Lemma 14,

$$\log |S| \geq k \sim \frac{x}{\log x},$$

while

$$\log |Y| \approx k \log s + (2 + \delta)s \log q \approx \frac{x^2}{\log x}.$$

Thus

$$\log |S| \approx \sqrt{\frac{\log |Y|}{\log \log |Y|}},$$

as desired.

Now we will derive constraints on $m = |Y|$. Since $x \gg 1$, we have $m \gg 1$. On the other hand, we must have

$$p \geq Mq^s \geq q^{2s}L = \frac{8q}{\phi(q)}q^{(3+\delta)s} \sim 8e^\gamma \log x q^{(3+\delta)s} \approx (\log \log q)q^{(3+\delta)s}.$$

Since $k \geq \frac{x}{\log x} \left(1 - \frac{C}{\log x}\right)$ and $q \approx e^x$, we have

$$s^k \gg k^k \gg \left(\frac{x}{\log x}\right)^k \gg \frac{q}{q^{C/\log \log q}}.$$

Thus

$$|Y| \gg \frac{q^{(3+\delta)s}}{q^{C/\log \log q}}.$$

Thus to ensure $(\log \log q)q^{(3+\delta)s} \ll p$, it suffices to take $|Y| \leq p^{1-\varepsilon}$ for any $\varepsilon > 0$. \square

2.3. Quantitative lower bounds over \mathbb{C} . In this section, we prove the lower bound in Theorem 3 for $\mathbb{F} = \mathbb{C}$.

Theorem 15. *For all $0 < \alpha < 1$ there exists an absolute constant $N_0 \geq 0$ such that for all $N \geq N_0$ there is a subset $Y \subseteq \mathbb{C}$ with that $|Y| \geq N$ and a set S of lines in general position that are α -rich in $Y \times Y$ and satisfy*

$$\log |S| \approx_\alpha \sqrt{\frac{\log |Y|}{\log \log |Y|}}.$$

The proof of Theorem 15 is an application of a *rectification theorem* of Grosu [18], which allows us to embed small subsets of \mathbb{F}_p into \mathbb{C} while preserving algebraic equations of low complexity. In particular, Grosu's theorem allows us to embed the counterexamples constructed in Theorem 11 into \mathbb{C}^2 . This seems to be the first time that Grosu's theorem has been used to prove a counterexample to a statement over \mathbb{C} , rather than to prove a positive statement for very small subsets of \mathbb{F}_p .

Before we state Grosu's theorem, we need some definitions. A polynomial $f \in \mathbb{Z}[x_1, \dots, x_n]$ is k -bounded if $\deg(f) \leq k$ and the sum of the absolute values of the coefficients of f are bounded by k . Given rings R_1 and R_2 and subsets $A = \{a_1, \dots, a_n\} \subseteq R_1$ and $B \subseteq R_2$, we call a bijection $\phi: A \rightarrow B$ a *Freiman ring isomorphism of order k* (or F_k -ring isomorphism) if for any k -bounded $f \in \mathbb{Z}[x_1, \dots, x_n]$ we have

$$f(a_1, \dots, a_n) = 0 \iff f(\phi(a_1), \dots, \phi(a_n)) = 0.$$

Theorem 16 (Grosu). *Let $k \geq 2$ be an integer, let p be a prime, and let A be a subset of \mathbb{F}_p . If $|A| < \log_2 \log_{2k} \log_{2k^2} p - 1$, then there exists a subset $A' \subseteq \mathbb{C}$, and a homomorphism $\phi_p: \mathbb{Z}[A'] \rightarrow \mathbb{F}_p$ such that ϕ_p is an F_k -ring homomorphism between A' and A .*

Grosu used Theorem 16 to prove that incidence bounds for points and lines in \mathbb{C}^2 can be applied to small sets of points and lines in \mathbb{F}_p^2 [18, Theorem 10]. We give a variation on this argument that guarantees that lines in general position in \mathbb{C}^2 correspond to lines in general position in \mathbb{F}_p^2 .

Corollary 17. *Let p be a prime, let Y be a subset of \mathbb{F}_p , and let S be a set of lines in \mathbb{F}_p^2 in general position that are α -rich in $Y \times Y$ for some $0 < \alpha < 1$.*

If $|Y| + 2|S| + \binom{|S|}{3} < \log_2 \log_{14} \log_{98} p - 2$, then there exists a subset $Y' \subseteq \mathbb{C}$ and a set of lines S' in \mathbb{C}^2 that are in general position and α -rich in $Y' \times Y'$.

Proof. We will show that it suffices to construct a F_7 -ring isomorphism between a certain subset $A \subseteq \mathbb{F}_p$ and some subset $A' \subseteq \mathbb{C}$.

Suppose that the elements of S have the form $\ell_i(x) = a_i x + b_i$. If ℓ_i, ℓ_j, ℓ_k are distinct lines that intersect in a common point, then the matrix

$$\begin{pmatrix} a_i & b_i & 1 \\ a_j & b_j & 1 \\ a_k & b_k & 1 \end{pmatrix}$$

is singular. By hypothesis, the lines of S are in general position, so the numbers

$$(13) \quad d_{ijk} := \det \begin{pmatrix} a_i & b_i & 1 \\ a_j & b_j & 1 \\ a_k & b_k & 1 \end{pmatrix}$$

are non-zero.

Let A be the union of Y , $\{a_i\}$, $\{b_i\}$, $\{d_{ijk}\}$, and $\{0\}$. Then by hypothesis

$$(14) \quad |A| \leq |Y| + 2|S| + \binom{|S|}{3} + 1 < \log_2 \log_{14} \log_{98} p - 1.$$

For each line ℓ_i , we have at least $\alpha|Y|$ solutions to

$$(15) \quad y' = a_i y + b$$

with y, y' in Y . This equation is 3-bounded. The equation (13) is 7-bounded.

By (14), we may apply Theorem 16 to A to find a subset $A' \subseteq \mathbb{C}$ and a F_7 -ring homomorphism $\phi_p: \mathbb{Z}[A'] \rightarrow \mathbb{F}_p$ from A' to A .

Let $Y' \subseteq \mathbb{C}$ denote the set of elements in A' that map to Y under ϕ_p and let S' denote the set of lines defined by $\ell'_i(x) = a'_i x + b'_i$ where $\phi_p(a'_i) = a_i$ and $\phi_p(b'_i) = b_i$. Since ϕ_p is a bijection from A' to A , we have $|Y'| = |Y|$ and $|S'| = |S|$.

Since ϕ_p preserves (13) and (15), the lines of S' are in general position (since by bijectivity, no d_{ijk} is mapped to 0), and each line in S' is incident to at least $\alpha|Y'|$ points of $Y' \times Y'$. \square

We are now ready to prove Theorem 15.

Proof of Theorem 15. Without loss of generality, we may assume that $|S| < N^{1/3}$. Choose a prime p so that

$$(16) \quad 5N \leq \log_2 \log_{14} \log_{98} p - 2.$$

Since $N_0 \leq N \leq p^{1/2}$, if N_0 is sufficiently large (depending on α), then by Theorem 11 there is a subset $Y \subseteq \mathbb{F}_p$ of size $\approx_\alpha N$ and a set S of lines in \mathbb{F}_p^2 in general

position and α -rich in $Y \times Y$ such that

$$\log |S| \approx_\alpha \sqrt{\frac{\log |Y|}{\log \log |Y|}}.$$

By (16) we have

$$|Y| + 2|S| + \binom{|S|}{3} \leq 5N \leq \log_2 \log_{14} \log_{98} p - 2,$$

so by Corollary 17 we may embed Y into \mathbb{C} and S into \mathbb{C}^2 . \square

3. UPPER BOUNDS FOR RICH LINES IN GRIDS

In this section, we prove two upper bounds for the number of rich lines in a $N \times N$ grid in \mathbb{F}^2 , and an asymmetric sum-product estimate over \mathbb{F} , where $\mathbb{F} = \mathbb{C}$ or $\mathbb{F} = \mathbb{F}_p$. If $\mathbb{F} = \mathbb{F}_p$, we need an additional constraint to rule out trivial counter-examples: the grid $\mathbb{F}_p \times \mathbb{F}_p$ has p^2 1-rich lines, and \mathbb{F}_p does not grow under addition or multiplication.

These theorems are all consequences of Theorem 4, which is a general inverse theorem for rich lines in grids. Theorem 4 is an immediate corollary of Theorem 21, which is an inverse theorem for rich affine transformations. The difference between Theorems 4 and 21 is a matter of language, and we give a dictionary between geometric and algebraic terminology in Section 3.1.

First we state the upper bound for α -rich lines in a $N \times N$ grid where $\alpha = N^{-\delta}$, which generalizes Theorem 5 to sets of lines of size N^ε for any $\varepsilon > 0$, as well as to points and lines defined over \mathbb{C} or \mathbb{F}_p .

Theorem 18 (Upper bound, polynomial density). *For all $\varepsilon > 0$ and $0 < \gamma < 1$, there is a $\delta > 0$ such the following holds for all $N > 0$.*

Let L be a set of N^ε lines in \mathbb{F}^2 that are $N^{-\delta}$ -rich in an $N \times N$ grid.

- *If $\mathbb{F} = \mathbb{C}$, then there is a subset $L' \subseteq L$ of size $|L'| \gg |L|^{1-\gamma}$ such that the lines of L' are either parallel or concurrent.*
- *If $\mathbb{F} = \mathbb{F}_p$, the same conclusion holds, provided that $N \ll p^{1-O(\gamma\varepsilon)}$.*

Further, we may take $\delta = 1/(J2^J)$, where $J \approx \gamma\varepsilon$.

Theorem 18 immediately implies the main theorem of [1] (Theorem 7), since if the lines of L are in general position, then $|L'| \leq 2$, which yields a contradiction for N sufficiently large.

Next we consider α -rich lines in an $N \times N$ grid where α is fixed.

Theorem 19 (Upper bound, constant density). *For all $0 < \alpha < 1$ there is a constant $C = C(\alpha) > 0$ such that the following holds for all $N > 0$.*

Let L is a set of lines in \mathbb{F}^2 that are in general position and are α -rich in an $N \times N$ grid.

- *If $\mathbb{F} = \mathbb{C}$, then $|L| \ll_\alpha N^{C/\log \log N}$.*
- *If $\mathbb{F} = \mathbb{F}_p$, then same conclusion holds, provided that $N^{1+\log(2/\alpha)/\log \log N} \leq p$.*

Theorem 19 proves the upper bounds stated in Theorem 3.

We will prove the following asymmetric sum-product result, which immediately implies Theorem 9.

Theorem 20 (Asymmetric sum-product theorem). *Suppose that $A, B, C \subseteq \mathbb{F}$ are finite. Let $J > 0$ be a positive integer and let $0 < K \leq \frac{1}{2}|A|^{1/2^J}$ be a parameter.*

If $\mathbb{F} = \mathbb{C}$, then either

$$(17) \quad |AC| + |A + B| > K|A|,$$

or

$$(18) \quad \min(|B|, |C|) \ll K^{C2^J} |A|^{C/J}.$$

If $\mathbb{F} = \mathbb{F}_p$, the same dichotomy holds, provided that $|A| \leq (2K)^{-2^J} p$.

Choosing $2K = |A|^{\frac{1}{J2^J}}$ proves Theorem 9 with $\varepsilon = 1/J$, since (18) cannot hold for this choice of K .

Theorems 18, 19, and 20 are special cases of the following general inverse theorem for rich lines in grids, which we stated in the introduction.

Theorem 4. *There is an absolute constant $C > 0$ such that the following holds. Let Y be a finite subset of \mathbb{F} and let L be a set of α -rich lines in $Y \times Y$. Let $J > 0$ be an integer such that $(\alpha/2)^{2^J} \geq 1/|Y|$.*

If $\mathbb{F} = \mathbb{C}$, then there is a subset $L' \subseteq L$ such that

- (1) *the lines of L' are either parallel or concurrent, and*
- (2) $|L'| \gg \left(\frac{\alpha}{2}\right)^{C2^J} |Y|^{-C/J} |L|$.

If $\mathbb{F} = \mathbb{F}_p$, then the same conclusion holds, provided that $|Y| \leq (\alpha/2)^{2^J} p$.

In turn, Theorem 4 is a simple translation of an *algebraic inverse theorem* for rich affine transformations.

We need some notation. If Y is a finite subset of \mathbb{F} , we let $\text{Sym}_\alpha(Y)$ denote the set of transformations g in $\text{Aff}(1, \mathbb{F})$ such that $|Y \cap gY| \geq \alpha|Y|$.

Theorem 21 (Inverse theorem for $\text{Aff}(1, \mathbb{F}) \curvearrowright \mathbb{F}$). *Let \mathbb{F} denote \mathbb{C} or \mathbb{F}_p . There exists an absolute constant $C > 0$ such that the following holds:*

Suppose that $Y \subseteq \mathbb{F}$ is finite, $0 < \alpha < 1$, and $A \subseteq \text{Sym}_\alpha(Y)$.

Let $J \geq 0$ be an integer such that $(\alpha/2)^{2^J} \geq 1/|Y|$, and if $\mathbb{F} = \mathbb{F}_p$, suppose that J also satisfies $|Y| \leq \left(\frac{\alpha}{2}\right)^{2^J} p$.

Then there is an element g in G and an abelian subgroup H of G such that

$$|A \cap gH| \gg \left(\frac{\alpha}{2}\right)^{C2^J} |Y|^{-C/J} |A|.$$

The significance of A containing many elements in an abelian subgroup is that the only way to have many rich transformations is by popular differences or popular ratios.

In the first subsection, we give a dictionary between the geometric language of rich lines and the algebraic language of symmetry sets, then prove Theorem 4. In the next subsection, we prove Theorems 18, 19, and 20. Theorem 21 is proved in the final subsection.

3.1. A geometric/algebraic dictionary and proof of Theorem 4. As we have said, $G = \text{Aff}(1, \mathbb{F})$ consists of transformations $x \mapsto ax + b$ with $a, b \in \mathbb{F}$ and $a \neq 0$. The group G acts on the *affine line* $X = \mathbb{F}$ by linear maps. If $g \in G$, Y is a finite subset of X , and $|Y \cap gY| \geq \alpha|Y|$, we say that g is an α -*approximate symmetry* of

Y . The collection of all α -approximate symmetries of a set is called a *symmetry set*

$$\text{Sym}_\alpha(Y) = \{g \in G : |Y \cap gY| \geq \alpha|Y|\}.$$

Symmetry sets were first defined in additive combinatorics in [37, Section 2.7]; symmetry sets for a general action of a group G on a set X are discussed in more detail in [26].

Every affine transformation in $\text{Aff}(1, \mathbb{F})$ corresponds to a line (its graph) in \mathbb{F}^2 . By convention, we ignore vertical lines, thus every line in \mathbb{F}^2 is the graph of transformation in $\text{Aff}(1, \mathbb{F})$.

Several properties of rich lines correspond to properties of approximate symmetries:

- (1) collections of rich lines in grids correspond to symmetry sets,
- (2) collections of *parallel lines* correspond to cosets of the *translation subgroup*,
- (3) collections of *concurrent lines* correspond to cosets of *homothety subgroups*.

To prove (1), simply note that if a line ℓ has the equation $y = ax + b$ then

$$(19) \quad |\ell \cap (Y \times Y)| \geq \alpha|Y| \iff |Y \cap (aY + b)| \geq \alpha|Y|.$$

To prove (2) and (3), we need a bit of background on the subgroups of the affine group.

Let τ_b denote the transformation $x \mapsto x + b$. The *translation subgroup* $U := \{\tau_b : b \in \mathbb{F}\}$ is a normal subgroup of G corresponding to translations of \mathbb{F} . (U is for “unipotent”.)

Let d_a denote the transformation $x \mapsto ax$. The *dilation subgroup* $T = \{d_a : a \in \mathbb{F}^*\}$ corresponds to dilations of \mathbb{F} about 0. In general, the stabilizer of a point x in \mathbb{F} under the action of $\text{Aff}(1, \mathbb{F})$ has the form $\text{Stab}(x) = gTg^{-1}$, where $g(0) = x$; $\text{Stab}(x)$ is the *homothety subgroup* of dilations about x .

The dilation subgroup and the homothety subgroups are the *maximal abelian subgroups* of G . (If H is abelian, either $H \subseteq U$ or there is an element $x \in H \setminus U$, and H is contained in the centralizer of x , which is a homothety subgroup.) We will usually say “abelian subgroup” rather than saying “dilation or homothety subgroup”.

For $x, y \in \mathbb{F}$, the set of transformations $\text{Trans}(x, y)$ sending x to y has the form $\text{Trans}(x, y) = gTh$, where $h(y) = 0$ and $g(0) = x$. We call $\text{Trans}(x, y)$ the *transporter of x to y* ; it is a left coset of $\text{Stab}(x)$ and a right coset of $\text{Stab}(y)$.

If L is a set of (non-vertical) lines in \mathbb{F}^2 , let A_L denote corresponding set of affine transformations.

- Property (2) holds since the lines of L have common slope a if and only if the corresponding set of affine transformations A_L is contained in $d_a U$, and
- Property (3) holds since the lines of L are incident to a common point (x, y) in \mathbb{F}^2 if and only if A_L is contained in $\text{Trans}(x, y)$, which is a coset of a homothety subgroup.

Now we derive Theorem 4 from Theorem 21.

Proof of Theorem 4. Let L be a set of α -rich lines in $Y \times Y$ and let A denote the set of affine transformations corresponding to L .

By Theorem 21, if $(\alpha/2)^{2^J} \geq 1/|Y|$, and $|Y| \leq (\alpha/2)^{2^J} p$ in the case $\mathbb{F} = \mathbb{F}_p$, then there is an abelian subgroup $S \leq G$ and an element g in G such that

$$|A \cap gS| \gg \left(\frac{\alpha}{2}\right)^{C 2^J} |Y|^{-C/J} |A|.$$

Let L' denote the set of lines in L that correspond to elements of $A \cap gS$. By Properties 2 and 3, the lines of L' are either parallel or concurrent, and since $|L'| = |A \cap gS|$ and $|L| = |A|$, the desired lower bound holds. \square

3.2. Proof of Theorems 18, 19, and 20. In this section we prove Theorems 18, 19, and 20 using Theorem 4. The proofs of Theorems 18 and 19 simply consist of choosing parameters and checking that the hypotheses of Theorem 4 are satisfied. The proof of Theorem 20 is essentially the same as the proof of Corollary 8 presented in the introduction.

Proof of Theorem 18. Let $N = |Y|$. Let J be a positive integer such that $J > 2C/\gamma\varepsilon$, where C is the constant from Theorem 4. Choose $\delta = 1/(J2^J)$.

To apply Theorem 4 for $\alpha = N^{-\delta}$, we must check the constraints on α and J . Since

$$(20) \quad \left(\frac{\alpha}{2}\right)^{2^J} = \left(\frac{1}{2N^\delta}\right)^{2^J} = \frac{1}{2^{2^J} N^{1/J}},$$

for N sufficiently large, we have $(\alpha/2)^{2^J} \geq 1/N = 1/|Y|$. If $\mathbb{F} = \mathbb{F}_p$, we must check the additional constraint $|Y| \leq (\alpha/2)^{2^J} p$. Since

$$\left(\frac{\alpha}{2}\right)^{2^J} p \gg_{\gamma, \varepsilon} N^{-\gamma\varepsilon/2C} p,$$

the additional constraint follows from the addition hypothesis $N \ll p^{1-O(\gamma\varepsilon)}$ when $\mathbb{F} = \mathbb{F}_p$.

Thus in either case, we may apply Theorem 4 to find a subset $L' \subseteq L$ of either parallel or concurrent lines such that

$$|L'| \gg \left(\frac{\alpha}{2}\right)^{C 2^J} |Y|^{-C/J} |L| \gg_J N^{-C\delta 2^J} N^{-C/J} |L|.$$

To complete the proof, we must show that $|L'| \gg |L|^{1-\gamma}$, which follows from our choice of J and δ :

$$N^{C\delta 2^J} N^{C/J} \ll N^{\gamma\varepsilon} \leq |L|^\gamma.$$

\square

Proof of Theorem 19. Let $N = |Y|$ and set

$$J = \log_2 \left(\frac{\log_2 N}{\log_2 \log_2 N} \right).$$

Then $N^{1/2^J} = \log_2 N$, so $(\alpha/2)^{2^J} \geq 1/|Y|$ for N sufficiently large. Since

$$(21) \quad \left(\frac{\alpha}{2}\right)^{2^J} = N^{-\log_2(2/\alpha)/\log_2 \log_2 N},$$

the constraint $|Y| \leq (\alpha/2)^{2^J} p$ follows from the condition

$$N^{1-\log_2(2/\alpha)/\log_2 \log_2 N} \leq p.$$

Thus we may apply Theorem 4 to find a subset $L' \subseteq L$ of either parallel or concurrent lines such that

$$|L'| \gg \left(\frac{\alpha}{2}\right)^{C 2^J} |Y|^{-C/J} |L|.$$

Since the lines of L are in general position, we have $|L'| \leq 2$. Thus

$$|L| \ll \left(\frac{2}{\alpha}\right)^{C 2^J} N^{C/J}.$$

For N sufficiently large, $J \gg \log_2 \log_2 N$, by (21) we have

$$|L| \ll N^{C \frac{1 - \log(\alpha)}{\log \log N}}.$$

□

Proof of Theorem 20. Suppose that (17) is false. Let $Y = AC \cup (A + B)$. Then $|Y| \leq K|A|$.

Let L denote the set of lines of the form $y = c(x - b)$ with $b \in B$ and $c \in C$. Each line ℓ in L satisfies $|Y \cap \ell(Y)| \geq |A| \geq \frac{1}{K}|Y|$, hence L is a set of α -rich lines in $Y \times Y$ with $\alpha = 1/K$.

The constraints on K imply that $(\alpha/2)^{2^J} \geq 1/|Y|$ and $|Y| \leq (\alpha/2)^{2^J} p$, if $\mathbb{F} = \mathbb{F}_p$. Thus by Theorem 21, there is subset $L' \subseteq L$ consisting of either parallel or concurrent lines with size

$$|L'| \gg \left(\frac{\alpha}{2}\right)^{C 2^J} |Y|^{-C/J} |L|.$$

Since L contains at most $|B|$ parallel lines and at most $|C|$ concurrent lines, we have

$$\max(|B|, |C|) \gg \left(\frac{\alpha}{2}\right)^{C 2^J} |Y|^{-C/J} |B||C|,$$

hence

$$\min(|B|, |C|) \ll (2K)^{C 2^J} |Y|^{C/J}.$$

□

Remark. Theorem 20 can be proved directly from Theorem 21 by noting that the transformations $x \mapsto c(x - b)$ are contained in $\text{Sym}_\alpha(Y)$ for $\alpha = 1/K$.

3.3. Proof of Theorem 21. Theorem 21 follows from a general inverse theorem for groups actions, which is a group action version of (asymmetric) Balog-Szemerédi-Gowers theorem [26]. In addition to this general inverse theorem, we need two other inputs specific to the action of $\text{Aff}(1, \mathbb{F})$ on \mathbb{F} for $\mathbb{F} = \mathbb{C}$ and $\mathbb{F} = \mathbb{F}_p$:

- (1) a *product theorem* for $\text{Aff}(1, \mathbb{F})$, and
- (2) *bounds* for the size of $\text{Sym}_\alpha(Y)$.

3.3.1. Group action version of the (asymmetric) Balog-Szemerédi-Gowers theorem. First, we state the group action version of the Balog-Szemerédi-Gowers theorem from [26]. We simplify the statement slightly, and specialize to $\text{Aff}(1, \mathbb{F})$ acting on \mathbb{F} .

Theorem 22. *There is an absolute constant $C > 0$ such that the following holds.*

Let Y be a finite subset of \mathbb{F} and let A be a finite subset of $\text{Aff}(1, \mathbb{F})$. Given a number $0 < \alpha < 1$ and an integer $J \geq 0$, define

$$(22) \quad \alpha_J = 2 \left(\frac{\alpha}{2} \right)^{2^J} \quad \text{and} \quad K = \left(\frac{|\text{Sym}_{\alpha_J}(Y)|}{|A|} \right)^{1/J}.$$

If $A \subseteq \text{Sym}_\alpha(Y)$, then

(1) there is an element g_ in G and a finite subset $A_* \subseteq G$ such that*

$$(23) \quad g_*^{-1} A_* \subseteq \text{Sym}_{\alpha_J}(Y)$$

and

$$(24) \quad |A_*^3| \ll \left(\frac{K}{\alpha_J} \right)^C |A_*|,$$

(2) for any subset $S \subseteq G$ there is an element g in G such that

$$(25) \quad |A \cap gS| \gg \left(\frac{\alpha_J}{K} \right)^C \frac{|S \cap A_*|}{|A_*|} |A|.$$

Part (1) of Theorem 22 says that some symmetry set of Y contains a set A_* with small tripling, which will allow us to apply the product theorems, stated next, to find a coset S of an abelian subgroup such that $|A_* \cap S|$ is large. Part (2) of Theorem 22 then says that $|A \cap gS|$ is large as well, which gives us the desired structure in A .

3.3.2. Product theorems for $\text{Aff}(1, \mathbb{C})$ and $\text{Aff}(1, \mathbb{F}_p)$. The following product theorem is a special case of a product theorem for solvable groups of $GL_n(\mathbb{C})$, due to Breuillard and Green [6, Theorem 1.4’].

Theorem 23 (Product theorem for $\text{Aff}(1, \mathbb{C})$). *Fix $K \geq 1$. If A is a finite subset of $\text{Aff}(1, \mathbb{C})$ such that $|A^3| \leq K|A|$, there is a subset $A' \subseteq A$ with size $|A'| \geq K^{-C}|A|$ that is contained in a coset of an abelian subgroup of $\text{Aff}(1, \mathbb{C})$.*

Over \mathbb{F}_p , Helfgott has proved a similar theorem [20, Proposition 4.8].

Theorem 24 (Product theorem for $\text{Aff}(1, \mathbb{F}_p)$). *Let $G = \text{Aff}(1, \mathbb{F}_p)$, let U be the translation subgroup, and let $\pi: G \rightarrow G/U$ be the quotient map.*

For a subset $A \subseteq G$, if there is a constant $K \geq 1$ such that $|A^3| \leq K|A|$, then for an absolute constant $C > 0$ we have either

$$(26) \quad |A \cap T| \gg |A|,$$

$$(27) \quad |\pi(A)| \ll K^C,$$

or

$$(28) \quad K^C |A| \gg |\pi(A)|p.$$

Theorems 23 and 24 can be proved by combining the orbit-stabilizer theorem for sets [20, Lemma 4.1] with a pivot argument or sum-product theorem. For completeness, we include proofs of Theorems 23 and 24 in Appendix B, using the sum-product theorems from [30, 41].

Since $|\pi(A)|$ is the number of cosets of U needed to cover A , if (27) holds, then there is an element g in G such that $|A \cap gU| \gg K^{-C}|A|$. We also know that $|A| \ll |\text{Sym}_{\alpha_J}(Y)|$, and we will use this to draw a similar conclusion from (28) using the upper bounds for $|\text{Sym}_\alpha(Y)|$.

3.3.3. *Upper bounds for $|\text{Sym}_\alpha(Y)|$.* Finally, we quote upper bounds for the symmetry sets for the action of $\text{Aff}(1, \mathbb{F})$ on \mathbb{F} .

Theorem 25. *Let Y be a finite subset of \mathbb{F} and let α be greater than $2/|Y|$.*

If $\mathbb{F} = \mathbb{C}$, then

$$|\text{Sym}_\alpha(Y)| \ll \alpha^{-3}|Y|.$$

If $\mathbb{F} = \mathbb{F}_p$ and $|Y| \leq \frac{\alpha}{2}p$, then

$$|\text{Sym}_\alpha(Y)| \ll \alpha^{-4}|Y|.$$

See [26] for a proof of Theorem 25, which is based on the Szemerédi-Trotter theorem [35, 38, 42, 33] for $\mathbb{F} = \mathbb{C}$ or the Stevens-de Zeeuw bound [34] combined with some additional arguments [28] for $\mathbb{F} = \mathbb{F}_p$.

Remark. Weaker bounds than those of Theorem 25 suffice for the proof of Theorem 21. We give specifics after the proof. This is in contrast to Elekes' proof of Theorem 5, which depends crucially on having bounds for $|\text{Sym}_\alpha(Y)|$ that are linear in $|Y|$.

3.3.4. Proof of Theorem 21.

Proof of Theorem 21. The condition $(\alpha/2)^{2^J} \geq 1/|Y|$ implies that $\alpha_J \geq 2/|Y|$, and the condition $|Y| \leq (\alpha/2)^{2^J}p$ implies that $|Y| \leq \frac{1}{2}\alpha p$. Hence by Theorem 25 we have

$$(29) \quad K \leq |\text{Sym}_{\alpha_J}(Y)|^{1/J} \ll \left(\frac{\alpha}{2}\right)^{-C} |Y|^{1/J}.$$

By Theorem 22, there is a constant $C > 0$, an element g_* in G , and a subset A_* of $g_* \text{Sym}_{\alpha_J}(Y)$ such that

$$(30) \quad |A_*^3| \ll (\alpha_J^{-1}K)^C |A_*|.$$

Now, suppose that $\mathbb{F} = \mathbb{C}$. By (30) and Theorem 23, there is an element g in G and an abelian subgroup H of G such that

$$|A_* \cap gH| \gg (\alpha_J^{-1}K)^{-C} |A_*|.$$

By equation (25) of Theorem 22, there is an element g' in G such that

$$(31) \quad |A \cap g'gH| \gg \alpha_J^2 (\alpha_J^{-1}K)^{-C} \frac{|A_* \cap gS|}{|A_*|} |A_0| \gg \alpha_J^C |Y|^{-C/J} |A_0|.$$

Since $\alpha_J = 2(\alpha/2)^{2^J}$, the proof is complete.

If $\mathbb{F} = \mathbb{F}_p$, then we apply Theorem 24 in place of Theorem 23. If (26) or (27) hold, then the proof is the same as in the case of $\mathbb{F} = \mathbb{C}$, so suppose that (28) holds:

$$(32) \quad \left(\frac{K}{\alpha_J}\right)^C |A_*| \gg |\pi(A_*)|p.$$

Since $A_* \subseteq g_* \text{Sym}_{\alpha_J}(Y)$, by Theorem 25 we have

$$(33) \quad |A_*| \leq |\text{Sym}_{\alpha_J}(Y)| \ll \alpha_J^{-4}|Y| \ll \alpha_J^{-3}p.$$

Combining this with (32) we have

$$|\pi(A_*)| \ll \left(\frac{K}{\alpha_J}\right)^C,$$

which implies that there is an affine transformation g such that

$$|A_* \cap gU| \gg \left(\frac{\alpha_J}{K}\right)^C |A_*|.$$

The rest of the proof is the same as in (31). \square

Remark. Instead of using Theorem 25 to prove (29), we could have used the bound $|\text{Sym}_\alpha(Y)| \ll \alpha^{-2}|Y|^2$, which follows from the Cauchy-Schwarz inequality and holds for $\text{Aff}(1, \mathbb{F}) \curvearrowright \mathbb{F}$ for any field \mathbb{F} , or even the trivial bound $|\text{Sym}_\alpha(Y)| \leq |Y|^4$, which holds because $|Y|^2$ points support at most $|Y|^4$ lines containing at least two elements of the point set.

Equation (33) could be proved using Vinh's incidence bound [39], which can also be proved using only Cauchy-Schwarz [27].

APPENDIX A. PROOF OF GROUP ACTION BALOG-SZEMERÉDI-GOWERS

In this section, we sketch the proof of the group action version the asymmetric Balog-Szemerédi-Gowers theorem, which we recall here.

Theorem 22. *There is an absolute constant $C > 0$ such that the following holds.*

Let Y be a finite subset of \mathbb{F} and let A be a finite subset of $\text{Aff}(1, \mathbb{F})$. Given a number $0 < \alpha < 1$ and an integer $J \geq 0$, define

$$(34) \quad \alpha_J = 2 \left(\frac{\alpha}{2}\right)^{2^J} \quad \text{and} \quad K = \left(\frac{|\text{Sym}_{\alpha_J}(Y)|}{|A|}\right)^{1/J}.$$

If $A \subseteq \text{Sym}_\alpha(Y)$, then

(1) there is an element g_ in G and a finite subset $A_* \subseteq G$ such that*

$$(35) \quad g_*^{-1} A_* \subseteq \text{Sym}_{\alpha_J}(Y)$$

and

$$(36) \quad |A_*^3| \ll \left(\frac{K}{\alpha_J}\right)^C |A_*|,$$

(2) for any subset $S \subseteq G$ there is an element g in G such that

$$(37) \quad |A \cap gS| \gg \left(\frac{\alpha_J}{K}\right)^C \frac{|S \cap A_*|}{|A_*|} |A|.$$

To understand how our method works, we will first revisit Elekes' proof of Theorem 5. The key idea is that *symmetry sets behave weakly like groups*. In fact, $\text{Sym}_1(Y)$ is a group: it is the stabilizer of Y under the induced action of on subsets of X . For $\alpha < 1$, a weak form of multiplicative closure holds.

Proposition 26 (Approximate multiplicative closure). *If S is a non-empty subset of $\text{Sym}_\alpha(Y)$, then there exists a relation $E \subseteq S^{-1} \times S$ such that*

$$|E| \geq \frac{\alpha^2}{2} |S|^2 \quad \text{and} \quad S^{-1} \overset{E}{\cdot} S \subseteq \text{Sym}_{\frac{\alpha^2}{2}}(Y).$$

Further, $(S^{-1} \overset{E}{\cdot} S)^{-1} = S^{-1} \overset{E}{\cdot} S$.

This is [26, Proposition 3], which is a straightforward generalization of [37, Lemma 2.33], which follows easily from Cauchy-Schwarz.

To prove that Theorem 5 follows from a product theorem, such as Theorem 6, we combine Proposition 26 with the upper bounds of Theorem 25.

Proposition 27. *Let \mathbb{F} be a field, and let $G = \text{Aff}(1, \mathbb{F})$ act on $X = \mathbb{F}$ by affine transformations. Let $A \subseteq G$ and $Y \subseteq X$ be finite subsets such that $A \subseteq \text{Sym}_\alpha(Y)$ and $|A| \geq |Y|$. Then there is a subset $E \subseteq A \times A$ such that $|E| \geq \frac{\alpha^2}{2}|A|^2$ and*

- (1) *if $\mathbb{F} = \mathbb{C}$, then $|A^{-1} \cdot^E A| \ll \alpha^{-6}|A|$,*
- (2) *if $\mathbb{F} = \mathbb{F}_p$ and $|Y| \leq \frac{1}{2}\alpha|Y|$, then $|A^{-1} \cdot^E A| \ll \alpha^{-8}|A|$.*

Proof. By Proposition 26, there is a subset $E \subseteq A \times A$ such that $|E| \geq \frac{\alpha^2}{2}|A|^2$ and

$$A^{-1} \cdot^E A \subseteq \text{Sym}_{\alpha^2/2}(Y).$$

By Theorem 25, if $\mathbb{F} = \mathbb{C}$,

$$|A^{-1} \cdot^E A| \leq |\text{Sym}_{\alpha^2/2}(Y)| \ll \alpha^{-6}|Y| \leq \alpha^{-6}|A|,$$

while if $\mathbb{F} = \mathbb{F}_p$ and $|Y| \leq \frac{1}{2}\alpha p$,

$$|A^{-1} \cdot^E A| \leq |\text{Sym}_{\alpha^2/2}(Y)| \ll \alpha^{-8}|Y| \leq \alpha^{-8}|A|.$$

□

Now we will prove the following theorem, in the spirit of Elekes' Theorem 5.

Theorem 28. *If N lines are α -rich in a $N \times N$ grid in \mathbb{C}^2 , then either*

- (1) *$C\alpha^C N$ lines are parallel, or*
- (2) *$C\alpha^C N$ lines are concurrent,*

where $C > 0$ is a constant independent of α and N .

The same holds for \mathbb{F}_p^2 , provided that $N \leq \frac{1}{2}\alpha p$.

To prove Theorem 28, we need the Balog-Szemerédi-Gowers theorem. The following version [26, Lemma 34], is essentially contained in [36].

Theorem 29. *If A and B are finite subsets of a group G and $E \subseteq A \times B$ is a relation such that*

$$|E| \geq \alpha|A||B| \quad \text{and} \quad |A \cdot^E B| \leq K|A|^{1/2}|B|^{1/2},$$

where $\alpha \in (0, 1]$ and $K > 0$, then there is an element a in A and a subset $S \subseteq a^{-1}A$ such that

$$|S| \gg \left(\frac{\alpha}{K}\right)^C |A| \quad \text{and} \quad |S^3| \ll \left(\frac{K}{\alpha}\right)^C |S|,$$

where C is an absolute constant.

Proof. Let \mathbb{F} denote \mathbb{C} or \mathbb{F}_p , let Y be a finite subset of \mathbb{F} , and suppose that $A \subseteq \text{Sym}_\alpha(Y)$. By Proposition 26, there is a subset $E \subseteq A^{-1} \times A$ such that

$$|E| \geq \frac{\alpha^2}{2}|A|^2 \quad \text{and} \quad |A^{-1} \cdot^E A| \ll \alpha^{-8}|A|.$$

By Theorem 29, there is an element a of A and a subset S of $\text{Aff}(1, \mathbb{F})$ such that $S \subseteq aA^{-1}$,

$$|S| \gg \alpha^{-C}|A|, \quad \text{and} \quad |S^3| \ll \alpha^{-C}|S|.$$

Now, as in the proof of Theorem 21, we may apply Theorem 23 or Theorem 24, depending on $\mathbb{F} = \mathbb{C}$ or $\mathbb{F} = \mathbb{F}_p$, to deduce that there is an abelian subgroup H of $\text{Aff}(1, \mathbb{F})$ such that $|S \cap gH| \gg \alpha^{-C}|S|$ for some g in $\text{Aff}(1, \mathbb{F})$. Since $S \subseteq aA^{-1}$

and $|S| \gg \alpha^{-C}|A|$, we have $|aA^{-1} \cap gH| \gg \alpha^{-C}|A|$, hence $|A \cap g^{-1}aH'| \gg \alpha^{-C}|A|$ for some subgroup H' conjugate to H .

To complete the proof, we translate to geometric language, as in the proof of Theorem 4. \square

It is a credit to Elekes' ingenuity that he proved Theorem 5 without the Balog-Szemerédi-Gowers theorem.

The assumption $|A| \geq |Y|$ is necessary to compare $|A^{-1} \cdot^E A|$ to $|A|$; if $|A| < |Y|$, then one may iterate Proposition 26 until we reach an iterated partial product set with small doubling. This strategy was used by Borenstein and Croot [2] to prove an analog of Elekes' results for small sets of lines (affine transformations). The analogy between Borenstein and Croot's work [2] and the asymmetric Balog-Szemerédi-Gowers theorem [37, Theorem 2.35], as observed by Helfgott [2], motivated Theorem 22.

To prove Theorem 22, we use a variation of Proposition 26. We use the notation \lesssim to hide logarithmic factors of α^{-1} and $|A|$.

Proposition 30 (Uniform approximate closure). *If A is a non-empty subset of $\text{Sym}_\alpha(Y)$ then there is a relation $E \subseteq A^{-1} \times A$ such that*

$$(38) \quad |E| \gtrsim \alpha^2 |A|^2,$$

$$(39) \quad r_E(x) \geq \frac{|E|}{2|A^{-1} \cdot^E A|} \quad \text{for all } x \text{ in } A^{-1} \cdot^E A,$$

$$(40) \quad A^{-1} \cdot^E A \subseteq \text{Sym}_{\frac{\alpha^2}{2}}(Y).$$

The proof of Proposition 30 is essentially the same as the proof of [37, Lemma 2.34]: combine Proposition 26 with a dyadic pigeonholing argument.

Proposition 30 implies that if a set S is dense in the product set $A^{-1} \cdot^E A$, then some translate of S is dense in A . Thus, if we find a “structured” subset of the product set $A^{-1} \cdot^E A$, we may bring that structure back to the original set A . More precisely, if A is a finite subset of G and $E \subseteq A^{-1} \times A$ satisfies (38) and (39), then for any subset S of G , there is an element a in A such that

$$(41) \quad \frac{|A \cap aS|}{|A|} \gtrsim \alpha^2 \frac{|(A^{-1} \cdot^E A) \cap S|}{|A^{-1} \cdot^E A|}.$$

Now we sketch the proof of Theorem 22.

Proof of Theorem 22. Let $A_0 = A$ and $\alpha_0 = \alpha$. By Proposition 30, there is a subset $E_0 \subseteq A_0^{-1} \times A_0$ such that (38), (39), and (40) hold. Define $A_1 := A_0^{-1} \cdot^{E_0} A_0$. By (41), for any subset S of $\text{Aff}(1, \mathbb{F})$, there is an element a_0 in A_0 such that

$$\frac{|A_0 \cap a_0 S|}{|A_0|} \gtrsim \alpha_0^2 \frac{|A_1 \cap S|}{|A_1|}.$$

Since $A_1 \subseteq \text{Sym}_{\alpha_1}(Y)$, where $\alpha_1 = \alpha_0^2/2$, we may iterate this process to find a sequence of numbers

$$\alpha_0 > \alpha_1 > \cdots > \alpha_J > 0$$

such that $\alpha_{j+1} = \alpha_j^2/2$, and a sequence of sets $A_j \subseteq \text{Aff}(1, \mathbb{F})$ such that $A_j \subseteq \text{Sym}_{\alpha_j}(Y)$, and for any set S in $\text{Aff}(1, \mathbb{F})$, there is an element a_j in A_j such that

$$(42) \quad \frac{|A_j \cap a_j S|}{|A_j|} \gtrsim \alpha_j^2 \frac{|A_j \cap S|}{|A_j|}.$$

Now for the key step: setting $K^J = |A_J|/|A_0|$, we have

$$K^J = \frac{|A_J|}{|A_0|} = \prod_{j=0}^{J-1} \frac{|A_{j+1}|}{|A_j|},$$

so by the pigeonhole principle, there is an index $0 \leq j \leq J-1$ such that $|A_{j+1}| \leq K|A_j|$. That is,

$$|A_j^{-1} \cdot^{E_j} A_j| \leq K|A_j|.$$

Since $|E_j| \gtrsim \alpha_j^2 |A_j|$, we can now apply the Balog-Szemerédi-Gowers theorem, as in the proof of Theorem 28, to find a subset S of $a_j A_j^{-1}$ such that

$$|S \cap a_j A_j^{-1}| \gg \left(\frac{\alpha_j}{K}\right)^C |A_j| \quad \text{and} \quad |S^3| \ll \left(\frac{K}{\alpha_j}\right)^C |S|.$$

If we wished to prove Theorem 21 directly, we would now apply a product theorem to find an abelian subgroup of $\text{Aff}(1, \mathbb{F})$ with large overlap with S .

Instead, we simply assume that there is some set H such that $|S \cap H| \gg (\alpha_j/K)^C |S|$. Iterating (42) yields an element g in G such that

$$\frac{|A_0 \cap gS|}{|A_0|} \gtrsim (\alpha_0 \cdots \alpha_j)^2 \frac{|A_j \cap S|}{|A_j|}.$$

Since $\alpha_j = 2(\alpha/2)^{2^j} \geq 2(\alpha/2)^{2^J}$, this completes the proof of Theorem 22. \square

APPENDIX B. PRODUCT THEOREMS FOR $\text{Aff}(1, \mathbb{F})$

Let U be a subgroup of a group G , and let $\pi: G \rightarrow G/U$ be the quotient map. For a subset A of G , let A/U denote the image of A under π ; that is, A/U is the set of left cosets of U of the form aU with a in A .

Recall that if $G = \text{Aff}(1, \mathbb{F})$, then a maximal torus T is a subgroup conjugate to the diagonal subgroup, and the unipotent subgroup U consists of upper triangular matrices with 1's on the diagonal. Every abelian subgroup of $\text{Aff}(1, \mathbb{F})$ is either contained in the unipotent subgroup U or a maximal torus.

The following is a specialization of [6, Theorem 1.4'] to $\text{Aff}(1, \mathbb{C})$.

Theorem 31 (Product theorem for $\text{Aff}(1, \mathbb{C})$). *If A is a subset of $\text{Aff}(1, \mathbb{C})$ such that $|A^3| \leq K|A|$, then either $\geq |A|/3$ elements of A are contained in a torus, or*

$$K^{10}|A| \gg |A/U|^{1/2}|A|,$$

hence there is an element g in G such that $|A \cap gU| \gg K^{-20}|A|$.

Theorem 31 says that if A is not contained in a torus, then either A is covered by a small number of cosets of U (so that A/U is small), or A grows under multiplication: $|A^3| \gg |A/U|^{1/20}|A|$.

The next theorem is a slight quantitative improvement of the product theorem for $\text{Aff}(1, \mathbb{F}_p)$ that appears in [20].

Theorem 32 (Product theorem for $\text{Aff}(1, \mathbb{F}_p)$). *If A is a subset of $\text{Aff}(1, \mathbb{F}_p)$ such that $|A^3| \leq K|A|$, then either there exists an element a_0 and a maximal torus T such that*

$$|(a_0^{-1}A) \cap T| \gg K^{-10}|A|,$$

or

$$K^{10}|A| \gg |A/U|^{1/2}|A|,$$

or

$$K^{10}|A| \gg |A/U|p.$$

B.1. Technical lemma. The following lemma contains the common elements of the proofs of Theorem 31 and Theorem 32.

Lemma 33. *If \mathbb{F} is a field and A is a finite subset of $\text{Aff}(1, \mathbb{F})$, then either more than one third of the elements of A are contained in an abelian subgroup, or there exists an x in A such that $|x^A x^{-1}| = |[A, x]| > 1$.*

Further there is an a_0 in A such that if $S := x^A x^{-1} \subseteq U$ and $T := (a_0^{-1}A) \cap C(x)$ then

$$|S||T| \geq |A| \quad \text{and} \quad |T| \leq |A/U|.$$

In addition, if $|A^3| \leq K|A|$, then

$$K^{10}|A| \gg |A/U| \cdot |B - BC|,$$

where $|B| = |S|$ and $|C| = |T|$.

The proof of Lemma 33 requires the following version of the orbit-stabilizer theorem for sets, rather than for groups [20] and Ruzsa's triangle inequality.

Lemma 34. *Suppose $G \curvearrowright X$, $x \in X$, and $A \subseteq G$ is finite. Then there exists a_0 in A such that*

$$(43) \quad |(a_0^{-1}A) \cap \text{Stab}(x)| \geq \frac{|A|}{|A(x)|},$$

and for all finite sets $B \subseteq G$,

$$(44) \quad |BA| \geq |A \cap \text{Stab}(x)||B(x)|.$$

Proposition 35 (Ruzsa triangle inequality). *If A, B, C are finite subsets of a group, then*

$$|AC^{-1}| \leq \frac{|AB^{-1}||BC^{-1}|}{|B|}.$$

Proof of Lemma 33. Suppose that at most $|A|/3$ elements of A are contained in an abelian subgroup. Then at least $2|A|/3$ elements of A are not contained in the unipotent group U , so without loss of generality, we may assume that A does intersect the unipotent group U . (That is, we will use A to denote $A \setminus U$.)

We still know that half of the elements of A are not contained in an abelian subgroup, thus there exists an x in A such that

$$(45) \quad |x^A x^{-1}| = |[A, x]| > 1.$$

Otherwise, $axa^{-1}x^{-1} = e$ for all a, x in A , which implies that the subgroup generated by A is abelian.

The set $x^A = \{axa^{-1} : a \in A\}$ is the orbit of x under the action of G on itself by conjugation; the stabilizer of x is denoted $C(x)$. Since $x \notin U$, we know that $C(x)$

is conjugate to the diagonal subgroup of $\text{Aff}(1, \mathbb{F})$; in particular, the only element of U fixed by $C(x)$ under conjugation is the identity element.

By Lemma 34, there is an element a_0 in A such that

$$|(a_0^{-1}A) \cap C(x)| \geq \frac{|A|}{|x^A|}.$$

Let T denote $a_0^{-1} \cap C(x)$.

Now, if $S = [A, x] = x^A \cdot x^{-1}$, then $|S| = |x^A|$; by (45) we know $|S| > 1$, so S contains an element of U besides the identity. Since $|T| = |(a_0^{-1}A) \cap C(x)|$, the previous equation can be restated as

$$|S||T| \geq |A|.$$

In addition, note that $|T| \leq |A/U|$, where A/U is the image of A under the quotient map $\pi: G \rightarrow G/U$. The inequality $|T| \leq |A/U|$ follows since π is injective when restricted to a torus.

Let S^T denote the image of S under the action of T by conjugation. Since $S \subseteq U$ and U is preserved by conjugation, we have $S \cdot (S^T)^{-1} \subseteq U$.

Let

$$B = \{z: \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix} \in S, z \neq 0\}$$

and let

$$C = \{a: \exists b \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in T\}.$$

Then

$$|S \cdot (S^T)^{-1} \cap U| = |S \cdot (S^T)^{-1}| \geq |B - BC|,$$

since conjugating $\begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}$ by $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ yields $\begin{pmatrix} 1 & az \\ 0 & 1 \end{pmatrix}$.

Clearly, $|B| \geq |S| - 1$ and since $\pi: G \rightarrow G/U$ is injective when restricted to T , we have $|C| = |T|$.

Note that

$$S \cdot (S^T)^{-1} = x^A x^{-1} ((x^A x^{-1})^T)^{-1} = x^A x^{-1} (x^{TA} x^{-1})^{-1} = x^A (x^{-1})^{TA}.$$

So that

$$S \cdot (S^T)^{-1} \subseteq Ax A^{-1} A^2 x^{-1} A^{-2} \subseteq A^2 A^{-1} A^2 A^{-3}.$$

By Lemma 34, we have

$$|A^3 A^{-1} A^2 A^{-3}| \geq |(A^2 A^{-1} A^2 A^{-3}) \cap U| |A/U| \geq |S \cdot (S^T)^{-1}| |A/U|.$$

By Proposition 35, if $|A^3| \leq K|A|$, then

$$|A^3 A^{-1} A^2 A^{-3}| \leq K^{10} |A|.$$

All together, we have

$$K^{10} |A| \geq |S \cdot (S^T)^{-1}| |A/U| \geq |A/U| |B - BC|,$$

as desired. \square

Note that if B contains only 0, then $|B - BC| = 1$; where as if B contains a non-zero element, then $|B - BC| \geq |C|$.

B.2. Proof of results over \mathbb{C} . The following theorem is an easy consequence of the Szemerédi-Trotter theorem, see [37, Exercise 8.3.3].

Proposition 36. *If A, B, C are finite subsets of \mathbb{C} , then*

$$|A + BC| \gg \sqrt{|A||B||C|}.$$

Proof of Theorem 31. If at least one third of the elements in H are contained in an abelian subgroup, then we are done.

Otherwise, by Lemma 33 and Proposition 36, we have

$$K^{10}|H| \gg |H/U||B - BC| \gg |H/U||B||C|^{1/2} = |H/U||S||T|^{1/2}.$$

Since $|T| \leq |H/U|$ and $|S||T| \geq |H|$, we have

$$K^{10}|H| \gg |H/U|^{1/2}|S||T| \geq |H/U|^{1/2}|H|.$$

□

B.3. Proof of results over \mathbb{F}_p . The following sum-product theorem is due to Roche-Newton, Rudnev, and Shkredov [30].

Proposition 37. *If $A, B, C \subseteq \mathbb{F}_p$ where p is prime, then*

$$|A + BC| \gg \min \left(\sqrt{|A||B||C|}, \frac{|A||B||C|}{M}, p \right),$$

where $M = \max(|A|, |B|, |C|)$.

In particular,

$$(46) \quad |B \pm BC| \gg \min \left(|B||C|^{1/2}, |B|^2, p \right).$$

Proof of the product theorem over \mathbb{F}_p . If A is contained in an abelian subgroup, then we are done.

Otherwise, by Lemma 33 and Proposition 37, we have

$$K^{10}|A| \gg |A/U||B - BC| \gg |A/U| \min \left(|B||C|^{1/2}, |B|^2, p \right).$$

If the minimum is $|B||C|^{1/2}$, then as in the previous proof, we have

$$K^{10}|A| \gg |A/U|^{1/2}|A|.$$

If the minimum is $|B|^2$, then we have

$$K^{10}|A| \gg |A/U||B|^2 \geq |A/U||S| \frac{|A|}{|T|} \geq |S||A|,$$

so $|S| \ll K^{10}$, which implies that

$$|(a_0^{-1}A) \cap C(x)| = |T| \gg \frac{|A|}{K^{10}}.$$

Finally, if the minimum is p , then we have

$$K^{10}|A| \gg |A/U|p.$$

□

REFERENCES

- [1] Gagik Amirkhanyan, Albert Bush, Ernest Croot, and Chris Pryby. Sets of rich lines in general position. *Journal of the London Mathematical Society*, 96(1):67–85, 2017.
- [2] Evan Borenstein and Ernie Croot. On rich lines in grids. *Discrete Comput. Geom.*, 43(4):824–840, 2010.
- [3] J. Bourgain. More on the sum-product phenomenon in prime fields and its applications. *Int. J. Number Theory*, 1(1):1–32, 2005.
- [4] Jean Bourgain and Alex Gamburd. Uniform expansion bounds for Cayley graphs of $SL_2(\mathbb{F}_p)$. *Ann. of Math.*, 167(2):625–642, 2008.
- [5] Emmanuel Breuillard. A brief introduction to approximate groups. In *Thin groups and superstrong approximation*, volume 61 of *Math. Sci. Res. Inst. Publ.*, pages 23–50. Cambridge Univ. Press, Cambridge, 2014.
- [6] Emmanuel Breuillard and Ben Green. Approximate groups, II: The solvable linear case. *Q. J. Math.*, 62(3):513–521, 2011.
- [7] Emmanuel Breuillard, Ben Green, and Terence Tao. Approximate subgroups of linear groups. *Geom. Funct. Anal.*, 21(4):774–819, 2011.
- [8] Emmanuel Breuillard, Ben Green, and Terence Tao. The structure of approximate groups. *Publ. Math. Inst. Hautes Études Sci.*, 116:115–221, 2012.
- [9] Ernie Croot and Vsevolod F Lev. Open problems in additive combinatorics. *Additive Combinatorics, CRM Proc. Lecture Notes*, 43:207–233, 2007.
- [10] György Elekes. On linear combinatorics. I. Concurrency—an algebraic approach. *Combinatorica*, 17(4):447–458, 1997.
- [11] György Elekes. On the number of sums and products. *Acta Arith.*, 81(4):365–367, 1997.
- [12] György Elekes. On linear combinatorics. II. Structure theorems via additive number theory. *Combinatorica*, 18(1):13–25, 1998.
- [13] György Elekes. SUMS versus PRODUCTS in number theory, algebra and Erdős geometry. In *Paul Erdős and his mathematics, II (Budapest, 1999)*, volume 11 of *Bolyai Soc. Math. Stud.*, pages 241–290. János Bolyai Math. Soc., Budapest, 2002.
- [14] György Elekes and Zoltán Király. On the combinatorics of projective mappings. *J. Algebraic Combin.*, 14(3):183–197, 2001.
- [15] P. Erdős and E. Szemerédi. On sums and products of integers. In *Studies in pure mathematics*, pages 213–218. Birkhäuser, Basel, 1983.
- [16] Nick Gill and Harald Andrés Helfgott. Growth in solvable subgroups of $GL_r(\mathbb{Z}/p\mathbb{Z})$. *Math. Ann.*, 360(1-2):157–208, 2014.
- [17] Frederick P. Greenleaf. *Invariant means on topological groups and their applications*. Van Nostrand Mathematical Studies, No. 16. Van Nostrand Reinhold Co., New York-Toronto, Ont.-London, 1969.
- [18] Codruț Grosu. \mathbb{F}_p is locally like \mathbb{C} . *J. Lond. Math. Soc. (2)*, 89(3):724–744, 2014.
- [19] H. A. Helfgott. Growth and generation in $SL_2(\mathbb{Z}/p\mathbb{Z})$. *Ann. of Math. (2)*, 167(2):601–623, 2008.
- [20] Harald A. Helfgott. Growth in groups: ideas and perspectives. *Bull. Amer. Math. Soc. (N.S.)*, 52(3):357–413, 2015.
- [21] Henryk Iwaniec and Emmanuel Kowalski. *Analytic number theory*, volume 53. American Mathematical Society Providence, 2004.
- [22] Maria Klawe. Non-existence of one-dimensional expanding graphs. In *22nd Annual Symposium on Foundations of Computer Science*. IEEE, Oct 1981.
- [23] Maria Klawe. Limitations on explicit constructions of expanding graphs. *SIAM J. Comput.*, 13(1):156–166, 1984.
- [24] A. Lubotzky and B. Weiss. Groups and expanders. In *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, volume 10. American Mathematical Soc., 1993.
- [25] Alexander Lubotzky. *Discrete groups, expanding graphs and invariant measures*, volume 125 of *Progress in Mathematics*. Birkhäuser Verlag, Basel, 1994. With an appendix by Jonathan D. Rogawski.
- [26] Brendan Murphy. Group action combinatorics. In prepration, 2017.
- [27] Brendan Murphy and Giorgis Petridis. A point-line incidence identity in finite fields, and applications. *Mosc. J. Comb. Number Theory*, 6(1):64–95, 2016.

- [28] Brendan Murphy, Giorgis Petridis, Oliver Roche-Newton, Misha Rudnev, and Ilya D. Shkredov. New results on sum-product type growth over fields, 2017.
- [29] László Pyber and Endre Szabó. Growth in linear groups. In *Thin groups and superstrong approximation*, volume 61 of *Math. Sci. Res. Inst. Publ.*, pages 253–268. Cambridge Univ. Press, Cambridge, 2014.
- [30] Oliver Roche-Newton, Misha Rudnev, and Ilya D. Shkredov. New sum-product type estimates over finite fields. *Adv. Math.*, 293:589–605, 2016.
- [31] Adam Sheffer. Incidences: Lower bounds (part 1).
- [32] Ilya D. Shkredov. Some remarks on the asymmetric sum-product phenomenon, 2017.
- [33] József Solymosi and Gábor Tardos. On the number of k -rich transformations. In *Proceedings of the twenty-third annual symposium on Computational geometry*, pages 227–231. ACM, 2007.
- [34] Sophie Stevens and Frank de Zeeuw. An improved point-line incidence bound over arbitrary fields. *arXiv preprint*, 2016.
- [35] Endre Szemerédi and William T. Trotter, Jr. Extremal problems in discrete geometry. *Combinatorica*, 3(3-4):381–392, 1983.
- [36] Terence Tao. Product set estimates for non-commutative groups. *Combinatorica*, 28(5):547–594, 2008.
- [37] Terence Tao and Van H. Vu. *Additive combinatorics*, volume 105 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2010. Paperback edition [of MR2289012].
- [38] Csaba D. Tóth. The Szemerédi-Trotter theorem in the complex plane. *Combinatorica*, 35(1):95–126, 2015.
- [39] Le Anh Vinh. On point-line incidences in vector spaces over finite fields. *Discrete Appl. Math.*, 177:146–151, 2014.
- [40] Benjamin Willson. Følner conditions and semidirect products related to amenability of semi-groups and groups. Master’s thesis, University of Alberta, 2006.
- [41] Esen Aksoy Yazici, Brendan Murphy, Misha Rudnev, and Ilya Shkredov. Growth Estimates in Positive Characteristic via Collisions. *Int. Math. Res. Not. IMRN*, 2016.
- [42] Joshua Zahl. A Szemerédi-Trotter type theorem in \mathbb{R}^4 . *Discrete Comput. Geom.*, 54(3):513–572, 2015.