Sharp Szemerédi-Trotter Constructions in the Plane

Larry Guth[a] Olivine Silier[b]

Submitted: Dec 1, 2021; Accepted: Jul 25, 2024; Published: Jan 17, 2025

Abstract

We present a new family of sharp examples for the Szemerédi-Trotter theorem. These are the first examples not based on a rectangular lattice. We also include an application to the discrete inverse Loomis-Whitney problem.

Mathematics Subject Classifications: 52C35, 52C10

1 Introduction

One formulation of the celebrated Szemerédi–Trotter theorem [25] provides a tight upper bound for the number of r-rich lines:

Theorem 1. (Szemerédi and Trotter) *Let $\mathcal{P}$ be a set of n points and let $\mathcal{L}_r$ be a set of lines we call r-rich that contain at least r points in $\mathcal{P}$, both in $\mathbb{R}^2$. Then*

$$|\mathcal{L}_r| = O\left(\frac{n^2}{r^3} + \frac{n}{r}\right).$$

This statement is equivalent to the statement in terms of point-line incidences [25], which goes as follows.

Theorem 2. (Szemerédi and Trotter) *Let $\mathcal{P}$ be a set of n points and let $\mathcal{L}$ be a set of m lines, both in $\mathbb{R}^2$. Then*

$$I(\mathcal{P}, \mathcal{L}) = O(m^{2/3}n^{2/3} + m + n).$$

The many variants of this theorem constitute an entire discipline called incidence theory. The theorem has also proved useful in other domains: its numerous applications range from problems in additive number theory to harmonic analysis [7, 8, 10, 18, 23]. Despite the community's interest [2, 14, 15, 24], the *inverse problem* : characterizing constructions that meet the Szemerédi-Trotter (mixed term) upper bound, remains widely

[a]Department of Mathematics, MIT, Cambridge, MA, USA. (lguth@math.mit.edu).
[b]Department of Mathematics, UC Berkeley, Berkeley, CA, USA (olivine_silier@berkeley.edu).

open. Although there has been recent progress for lines in general position on Cartesian product point sets, [11, 20] not much else is known.

Up to recently, only two constructions were known to match the non-linear term in Theorem 1 and Theorem 2. The first example, given by Erdős in 1946, is based on a square lattice. The second example, given by Elekes [15] in 2001, is based on a rectangular lattice. Adam Sheffer and the second author recently introduced the first infinite family of sharp Szemerédi-Trotter examples, which has the Erdős and Elekes constructions as limits [22]. In all of these examples, the point set is a *lattice*: a Cartesian product of two arithmetic progressions.

Every previous sharp example for the Szemerédi-Trotter theorem was found by starting with a Cartesian product of two arithmetic progressions and then applying a projective transformation and/or point-line duality. In this paper, we give a new sharp example which does not have this structure.

1.1 Our family of constructions.

We present the first sharp Szemerédi-Trotter family of non-lattice point-line constructions in $\mathbb{R}^2$: the x and y coordinates of the point set are a generalized arithmetic progression and for any richness r there is a maximal family of r-rich lines on the point set.

Theorem 3. *For any non-square integer k, any large enough N and $r \leqslant N$, let the point set $\mathcal{P} = A_N^2$ where $A_N = \left\{x_1 + x_2\sqrt{k}; x_1, x_2 \in \left[-\sqrt{N}, \sqrt{N}\right]\right\}$. Then there exists a set of r-rich lines $|\mathcal{L}_r|$ such that*

$$|\mathcal{L}_r| = \Theta\left(\frac{|\mathcal{P}|^2}{r^3} + \frac{|\mathcal{P}|}{r}\right).$$

Furthermore there are $\Theta(\frac{N^2}{r^2})$ many slopes and each slope corresponds to a family of $\Theta(\frac{N^2}{r})$ many parallel lines.

See Section 3 for the proof and the explicit construction of the line set.

1.2 Limitations and Motivation for the Construction

Our point set $\mathcal{P} = A_N^2$ is not a product of arithmetic progressions. It is a product of generalized arithmetic progressions (GAPs).

This construction is a generalization of the Erdős construction. We are interested in this case because it is a square grid: the x and y coordinate sets are the same. This is the most interesting case for our applications to inverse discrete Loomis-Whitney.

The choice of $\{1, \sqrt{k}\}$ as generators of GAP simplifies our analysis. If we were not working in a number field of degree 2 but instead tried to generalize this result to other number fields, it might still be possible to construct sharp examples but this would be more complicated.

This result cannot be generalized to a point set $A_N \times B_N$ because the number of incidences would be much lower than the desired sharp bound. Then the lines would instead be $O(\sqrt{N/M})$ rich. (See Remark in proof of Lemma 11).

Recent work by Currier [12] presents a set of sharp Szemerédi-Trotter examples where the point set is a Cartesian product of GAPs generated by the basis of general number fields over $\mathbb{Q}$. More incidences are made possible, and the analysis is simplified despite the more general choice of number fields, because Currier works on an 'unbalanced' grid of points that generalizes the simpler Elekes construction.

1.3 Application to Inverse Discrete Loomis-Whitney.

The Loomis-Whitney inequality [19] upperbounds the volume of an n dimensional set by the product of the areas of its "shadows": the $n-1$ dimensional coordinate projections.

Theorem 4. *Let m be the measure of an open subset O of the Euclidean n-space, and let $m_1, \ldots, m_n$ be the $(n-1)$-dimensional measures of the projections of O on the coordinate hyperplanes. Then*

$$m^{n-1} \leqslant \Pi_{i=1}^{n} m_i.$$

The many variations of this theorem constitute a rich field of study [3, 6, 4, 13]. These results also find applications in other domains from group theory [17] to the Kakeya problem in harmonic analysis [5]. Recently there has been much interest in the *inverse problem*: characterizing sets that provide sharp examples of the Loomis-Whitney inequality [9, 1]. We focus on the discrete variant of the inverse problem in $\mathbb{R}^2$: characterizing point configurations in the plane whose 1 dimensional projections are minimal. Classical Loomis-Whitney tells us that in the case of a point set in $\mathbb{R}^2$ of size n^2 (using affine transformations to map 2 arbitrary projection directions to the coordinate projections) the product of the size of these two projections is greater or equal to n^2. Equivalently, it is not possible for both projections to have size less than n.

Thus the natural inverse discrete Loomis-Whitney problem in the plane asks under which structural conditions of the point set of size n^2, and for which set of projection directions, all the one-dimensional projections have size $\Theta(n)$. Elementary arguments yield the following necessary and sufficient condition for square lattices:

Lemma 5. *Let the point set $\mathcal{P}$ be a section of the integer lattice of size $n \times n$. A one-dimensional projection of $\mathcal{P}$ has size $\Theta(n)$ if and only if the slope of the projection direction is an irreducible rational p/q such that $p, q = O(1)$.*

Note for any square lattice in the plane there exists an affine map which takes it to a square section of the integer square lattice. So up to affine transformation of the plane Lemma 5 holds for any square lattice.

Obtaining sharp constructions for the discrete inverse Loomis-Whitney problem in the plane for an $n \times n$ grid of points overlaps with finding sharp examples for Theorem 1 because finding a family of $\Theta(n)$ parallel $\Theta(n)$-rich lines yields a projection direction along which a constant fraction of the points have minimal projection size. We obtain the following application of Theorem 3:

Corollary 6. *For any non-square integer k, and large enough N, let the point set $\mathcal{P} = A_N^2$ where $A_N = \left\{x_1 + x_2\sqrt{k}; x_1, x_2 \in \left[-\sqrt{N}, \sqrt{N}\right]\right\}$. Then for any constant $p = O(1)$ there is a set of projections $\{\pi_i\}_{i=1}^{\Theta(p)}$ such that $|\pi_i(\mathcal{P})| = \Theta\big(\sqrt{p}n\big)$.*

1.4 Sharp example for Energy Bound.

Our constructions provide a new tight example for the following lemma which provide upperbounds for the additive energy of finite subsets of $\mathbb{R}$ [21]:

Lemma 7. *Let A, B and X be finite subsets of $\mathbb{R}$ such that $|X| \leqslant |A||B|$. Then*

$$\sum_{x\in X} E^+(A, xB) = O\big(|A|^{3/2}|B|^{3/2}|X|^{1/2}\big).$$

There exists a similar lemma for multiplicative energy [21]. The proofs of this lemma rely on an application of Theorem 1 so all of our sharp examples from Theorem 3 are also sharp for this lemma.

Lemma 8. *For any non-square integer k, and $M \leqslant N$ let $A_N = \left\{x_1 + x_2\sqrt{k}; x_1, x_2 \in \left[-\sqrt{N}, \sqrt{N}\right]\right\}$ and let $X = S \subset \frac{A_N}{A_N}$ be the slope set from Theorem 3. Then $|X| \leqslant |A_N|^2$ and*

$$\sum_{x\in X} E^+(A_N, xA_N) = \Theta\big(|A_N|^3|X|^{1/2}\big).$$

Note we can similarly construct a sharp example for the multiplicative energy version of the lemma.

2 Notation

Asymptotic notation is used throughout. We say $f(n) = O(g(n))$ if there exist constants $c, n_0 > 0$ such that $|f(n)| \leqslant c \cdot g(n)$ for all $n \geqslant n_0$. Likewise $f(n) = \Omega(g(n))$ if there exist constants $c, n_0 > 0$ such that $|f(n)| \geqslant c \cdot g(n)$ for all $n \geqslant n_0$. We say $f(n) = \Theta(g(n))$ if and only if $f(n) = O(g(n))$ and $f(n) = \Omega(g(n))$.

We also use the stronger notation $f(n) = o(g(n))$ if for all $\epsilon > 0$ there exists n_ϵ such that $|f(n)| \leqslant \epsilon \cdot g(n)$ for all $n \geqslant n_\epsilon$. Likewise we say $f(n) = \omega(g(n))$ if for all $\epsilon > 0$ there exists n_ϵ such that $|f(n)| \geqslant \epsilon \cdot g(n)$ for all $n \geqslant n_\epsilon$.

3 New Constructions

In this section we prove Theorem 3 and provide an explicit description of the line set. We first recall the statement of the theorem.

Theorem 3.
For any non-square integer k, any large enough N and $r \leqslant N$, let the point set $\mathcal{P} := A_N^2$

where $A_N = \left\{x_1 + x_2\sqrt{k}; x_1, x_2 \in \left[-\sqrt{N}, \sqrt{N}\right]\right\}$. *Then there exists a set of* r*-rich lines* $|\mathcal{L}_r|$ *such that*

$$|\mathcal{L}_r| = \Omega\left(\frac{|\mathcal{P}|^2}{r^3} + \frac{|\mathcal{P}|}{r}\right).$$

Furthermore there are $\Theta(\frac{N^2}{r^2})$ *many slopes and each slope corresponds to a family of* $\Theta(\frac{N^2}{r})$ *many parallel lines.*

Proof. We double count the number of incidences to obtain a lower bound on the size of the line set. This involves proving each of the lines are r-rich. Let $M = \frac{N}{r}$.

We first define the point set, slope set and line set. Note $|A_N| = \left(2\sqrt{N}\right)^2 = \Theta(N)$. Let the point set $\mathcal{P} = A_N^2$. Then we have $|\mathcal{P}| = \Theta(N^2)$.

Next we define the slope set:

$$S = \left\{\frac{p_1 + p_2\sqrt{k}}{q_1 + q_2\sqrt{k}}; |p_i|, |q_i| \in \left[c\sqrt{M}, \sqrt{M}\right], \gcd(p_1^2 - kp_2^2, q_1^2 - kq_2^2) = 1, \gcd(p_1, p_2) = 1\right\}.$$

for some absolute constant $3/4 < c < 1$. Then we define the line set

$$\mathcal{L} = \left\{y = s(x-a) + b; (a,b) \in A_{N/4}^2, s \in S\right\}.$$

Each point $(a,b) \in A_{N/4}^2 \subset \mathcal{P}$ has at least $|S|$ lines of $\mathcal{L}$ so $I(\mathcal{P}, \mathcal{L}) \geqslant |A_{N/4}^2||S| \gtrsim N^2|S|$.

Lemma 9. $|S| = \Theta(M^2)$

Proof. First note $|S| \leqslant \sqrt{M}^4 = M^2$.

To find a lower bound on $|S|$, we must first remove the quadruples (p_1, p_2, q_1, q_2) that do not satisfy the divisibility requirements. Let $T := (1-c)^4 M^2$. This is the total number of integer quadruples in the allowed range. Our goal is to show that there are a positive fraction of T many quadruples that satisfy the divisibility requirements.

First keep only quadruples where p_1, p_2 are of opposite parity and q_1 is odd. We are left with $T/4$ quadruples. Next remove quadruples where $d|\gcd(p_1, p_2)$ for some prime $d \geqslant 3$. We are left with $\geqslant T/4(1 - \sum_{d \geqslant 3\text{prime}} \frac{1}{d^2})$ many quadruples (since d and 2 are coprime so pairs (p_1, p_2) of opposite parity which are both divisible by d occur with frequency $1/d^2$ i.e. Chinese Remainder Theorem). Now, all our remaining quadruples satisfy the requirement $\gcd(p_1, p_2) = 1$.

We now handle the other divisibility criterion. If k is odd, recalling that p_1, p_2 have opposite parity we get that $p_1^2 - kp_2^2$ is odd. If k is even, recalling that q_1 is odd we get that $q_1^2 - kq_2^2$ is odd. Thus $2 \nmid \gcd(p_1^2 - kp_2^2, q_1^2 - kq_2^2)$.

We now remove quadruples such that $d \mid p_1^2 - kp_2^2$ and $d \mid q_1^2 - kq_2^2$ for some prime $d \geqslant 3$. First assume kp_2^2 is a quadratic residue mod d. (If kp_2^2 is not a quadratic residue, we do not need to remove this quadruple which only makes our bound stronger.) $\mathbb{F}_d$ is a field so the degree 2 equation in $\mathbb{F}_d : p_1^2 = kp_2^2 \mod d$ has at most two solutions for p_1, at most one of which is even, and at most one of which is odd. (Usually one of each unless the solution is 0 in which case it is a double root.) This is because if the first solution is x then the second solution is $d-x$ and d is odd. Note p_1, p_2 have opposite parity so there is only one solution for p_1 in terms of p_2. Similarly q_1 is odd so the analogous equation for q_i yields exactly one solution for the residue class of q_1 in terms of q_2.

Let d be some prime and p be a prime greater than 2. So far in the proof of this Lemma we have two divisibility conditions on p_1 and p_2 that would cause us to remove a quadruple containing that pair (p_1, p_2).

1. $d|\gcd(p_1, p_2)$ which can equivalently be written as $p_1 \equiv p_2 \mod d$. (Note if $d = 2$ this encodes the requirement that the remaining pairs p_1 and p_2 which we did not throw out have opposite parity.)

2. $d|p_1^2 - kp_2^2$ which can equivalently be written as $p_1 \equiv \pm\sqrt{kp_2^2} \mod p$ provided kp_2^2 is a quadratic residue mod p.

If d and p are distinct, then by the Chinese Remainder Theorem there is exactly one solution for p_1 modulo $d \cdot p$ to the system of equations 1) and 2). In other words, for each pair (p_1, p_2) the probability that we have to remove it because it satisfies Equation 1) is independent of the probability that we have to remove it because it satisfies Equation 2). If d and p are the same, then the solutions to Equation 1 are a subset of the solutions to Equation 2. We assume as before that the probability of a given pair of solving Equation 1 is independent of the probability of solving Equation 2, which means we will overestimate the number of pairs to be removed. If we were to account for this double counting, we would only be making our bound stronger. Same for q_1, q_2.

For each p_2 we must remove at most $\max(1, t_p/d)$ choices of p_1 where t_p is the total number of choices of p_1 in the range which satisfy the previous divisibility criteria. For each q_2 we must remove at most $\max(1, t_q/d)$ choices of q_1 where t_q is the total number of choices of q_1 in the range which satisfy the previous divisibility criteria. So to handle all $d \leqslant \sqrt{M}$ we remove a fraction of at most $\sum_{d \geqslant 3\text{prime}} \frac{1}{d^2}$ quadruples. To handle primes $\sqrt{M} \leqslant d \leqslant M$ we must remove at most 1 pair (p_1, q_1) for each pair $(p_2.q_2)$ per prime d. By the prime number theorem there are $\lesssim \frac{M}{\log(M)}$ primes in this range [26]. So we will have to remove $\lesssim \frac{M}{\log(M)}\sqrt{M}^2 \lesssim o(M^2)$ quadruples, which doesn't affect the leading exponent in our bound. So after accounting for the last divisibility criterion, we are left with $\geqslant T/4(1 - \sum_{d \geqslant 3\text{prime}} \frac{1}{d^2})^2$ quadruples.

Using a classical result [16] we find that $\sum_{d \geqslant 3\text{prime}} \frac{1}{d^2} < 1/4$ so at least $\frac{3^2}{4^3}T$ many quadruples satisfy the divisibility properties. Note that $\frac{3^2}{4^3}$ could be improved but we do not pursue optimizing the constants.

Recalling the definition of T (total number of quadruples) : at least $\frac{3^2}{4^3}(1-c)^4M^2$ quadruples satisfy the divisibility properties.

We now show each quadruple (p_1, p_2, q_1, q_2) in our range gives a unique fraction $\frac{p_1 + p_2\sqrt{k}}{q_1 + q_2\sqrt{k}}$.

$$\frac{p_1+p_2\sqrt{k}}{q_1+q_2\sqrt{k}}=\frac{r_1+r_2\sqrt{k}}{t_1+t_2\sqrt{k}}$$

We first solve for t_1 and t_2 by separating the integers and the factors of $\sqrt{k}$:

$$\begin{cases} t_1=\frac{1}{p_1^2-kp_2^2}[q_1(p_1r_1-kp_2r_2)+q_2k(p_1r_2-p_2r_1)] \\ t_2=\frac{1}{p_1^2-kp_2^2}[q_2(p_1r_1-kp_2r_2)+q_1(p_1r_2-p_2r_1)] \end{cases}$$

Recall $\gcd(p_1^2-kp_2^2,q_1^2-kq_2^2)\leqslant 1$ and all integers divide zero so $p_1^2-kp_2^2\neq 0$.

$$t_2q_1-t_1q_2=\frac{1}{p_1^2-kp_2^2}(q_1^2-kq_2^2)(p_1r_2-p_2r_1)$$

The left hand side is an integer and $\gcd(p_1^2-kp_2^2,q_1^2-kq_2^2)=1$ so $p_1^2-kp_2^2\mid p_1r_2-p_2r_1$.

However $p_1,p_2,r_1,r_2\in[c\sqrt{M},\sqrt{M}]$ so $|p_1^2-kp_2^2|\geqslant(kc-1)M$ and $|p_1r_2-p_2r_1|\leqslant(1-c^2)M$.

Recall $k\geqslant 2$ and $c\in(3/4,1)$. So $kc-1\geqslant 2c-1\geqslant 1/2>7/16\geqslant 1-c^2$. Thus $|p_1r_2-p_2r_1|<|p_1^2-kp_2^2|$ but $p_1^2-kp_2^2\mid p_1r_2-p_2r_1$ so $p_1r_2-p_2r_1=0$.

Furthermore $\gcd(p_1,p_2)=1$ so $r_1=fp_1$ and $r_2=fp_2$ for some integer f. $p_1,p_2,r_1,r_2\in[c\sqrt{M},\sqrt{M}]$ so $2p_1$ is already outside the range. Thus $(r_1,r_2)=(p_1,p_2)$ which also implies $(t_1,t_2)=(q_1,q_2)$. So the fraction corresponds to a unique quadruple in our range. So each quadruple that satisfies the above divisibility requirements contributes a unique element to S and we have found $|S|\geqslant\frac{3^2}{4^3}(1-c)^4M^2=\Omega(M^2)$.

$\square$

Recall $I(\mathcal{P},\mathcal{L})\geqslant N^2|S|$ and by Lemma 9: $I(\mathcal{P},\mathcal{L})\geqslant\frac{3^2}{4^3}(1-c)^4M^2N^2=\Omega(N^2M^2)$.

Lemma 10. $I(\mathcal{P},\mathcal{L})=\Omega(N^2M^2)$.

Lemma 11. *Each line in $\mathcal{L}$ has $\Theta\big(\frac{N}{M}\big)$ points in $\mathcal{P}$.*

Proof. We first show each line is $\Omega\big(\frac{N}{M}\big)$ rich. Let l be an arbitrary line in $\mathcal{L}$. There exist $s=\frac{p_1+p_2\sqrt{k}}{q_1+q_2\sqrt{k}}\in S$ and $(a,b)\in A^2_{N/4}$ such that l is the line $y-b=s(x-a)$. Then for all $x=a+(q_1+\sqrt{k}q_2)(a_1+\sqrt{k}a_2)$ we have $s(x-a)=(p_1+\sqrt{k}p_2)(a_1+\sqrt{k}a_2)=(p_1a_1+kp_2a_2)+(p_1a_2+p_2a_1)\sqrt{k}$ where $|p_i|\approx\sqrt{M}$. So for $a_i\in\left[0,\frac{\min_{i\in\{1,2\}}\sqrt{N}-|b_i|}{(k+1)\sqrt{M}}\right]$ each of the linearly independent terms have integer coefficients in the range $\max_{i\in 1,2}\left[-\sqrt{N}+|b_i|,\sqrt{N}-|b_i|\right]$.

So for all $\geqslant\left(\frac{\sqrt{N}}{(k+1)\sqrt{M}}\right)^2=\Omega\big(\frac{N}{M}\big)$ choices of a_1,a_2 in the above range, there exists $y\in B_N$ such that $y-b=s(x-a)$. Thus each line in $\mathcal{L}$ has $\geqslant\frac{N}{(k+1)^2M}=\Omega\big(\frac{N}{M}\big)$ points in $\mathcal{P}$.

Remark Here we rely on the set of $x-$coordinates and $y-$coordinates to be the same. Consider instead if the point set were instead $\mathcal{P}=A_N\times B_N$ where elements of A_N are $x_1+\sqrt{h}x_2$ and elements of B_N are $y_1+\sqrt{k}y_2$ and $\sqrt{h},\sqrt{k}$ are linearly independent on

$\mathbb{Q}$. Then for the equation $y-b=s(x-a)$ to be satisfied we need the $\sqrt{h}$ component and the $\sqrt{k}$ component to vanish. This requires $x-a$ to be a multiple of p (and then implies $y-b$ is a multiple of q). So there are $\leqslant max(x-a)/|p| = O(\sqrt{N}/\sqrt{M})$ possible multiples. These correspond to at most $O(\sqrt{\frac{N}{M}})$ points on the line which is significantly less than the sharp number of N/M points we get in the symmetric grid case.

Now we show each line in $\mathcal{L}$ has $O\big(\frac{N}{M}\big)$ points in $\mathcal{P}$. Let $(x,y)\in A_N^2=\mathcal{P}$ such that $(x,y)\in l$ for some line $l: y=\frac{p_1+p_2\sqrt{k}}{q_1+q_2\sqrt{k}}(x-a)+b\in\mathcal{L}$. Let $X_1+\sqrt{k}X_2=x-a$ and $Y_1+\sqrt{k}Y_2=y-b$. Note $X_1,X_2,Y_1,Y_2\in[-\frac{5}{4}\sqrt{N},\frac{5}{4}\sqrt{N}]$. We want to show there are $O(\frac{N}{M})$ solutions X_1,X_2,Y_1,Y_2 to $(X_1+\sqrt{k}X_2)(p_1+\sqrt{k}p_2)=(Y_1+\sqrt{k}Y_2)(q_1+\sqrt{k}q_2)$. Seperating the integer and $\sqrt{k}$ terms and solving for X_1 and X_2:

$$\begin{cases} X_1=\frac{1}{(p_1^2-kp_2^2)}[q_1(p_1Y_1-kp_2Y_2)+kq_2(p_1Y_2-p_2Y_1)] \\ X_2=\frac{1}{(p_1^2-kp_2^2)}[q_1(p_1Y_2-p_2Y_1)+q_2(p_1Y_1-kp_2Y_2)] \end{cases}$$

So $-q_2X_1+q_1X_2=\frac{(q_1^2-kq_2^2)}{(p_1^2-kp_2^2)}(p_1Y_2-p_2Y_1)$. Recall $\gcd(p_1^2-kp_2^2,q_1^2-kq_2^2)=1$ and the left hand side is an integer so there exists and integer j such that $p_1Y_2-p_2Y_1=j(p_1^2-kp_2^2)$. Thus $p_1Y_2\equiv jp_1^2 \mod (p_2)$ and $p_2Y_1\equiv jkp_2^2 \mod (p_1)$. Note $Y_1,Y_2\in[-\frac{5}{4}\sqrt{N},\frac{5}{4}\sqrt{N}]$ and $p_1,p_2\in[c\sqrt{M},\sqrt{M}]$ so $j\in[-\frac{5}{2(kc-1)}\frac{\sqrt{N}}{\sqrt{M}},\frac{5}{2(kc-1)}\frac{\sqrt{N}}{\sqrt{M}}]$ (recall $k\geqslant 2$ and $c\in(3/4,1)$). Furthermore p_1 and p_2 are coprime so each has a multiplicative inverse modulo the other. Thus $Y_1\equiv jkp_2 \mod (p_1)$ so there are $\leqslant\frac{5}{2}\frac{\sqrt{N}}{c\sqrt{M}}$ solutions for Y_1 for a given j.

So there are $\frac{25}{2c(kc-1)}\frac{N}{M}$ integer solutions (j,Y_1). Once we have fixed j and Y_1 there is at most one solution Y_2 and then at most one solution for X_1 at most one for X_2.

So each line in $\mathcal{L}$ has $\geqslant\frac{N}{(k+1)^2M}$ and $\leqslant\frac{25}{2c(kc-1)}\frac{N}{M}$ points in $\mathcal{P}$.

□

Each line in $\mathcal{L}$ has $\leqslant\frac{25}{2c(kc-1)}\frac{N}{M}$ points in $\mathcal{P}$ so $I(\mathcal{P},\mathcal{L})\leqslant\frac{25}{2c(kc-1)}\frac{N}{M}|\mathcal{L}|$. Combining with Lemma 10: $I(\mathcal{P},\mathcal{L})\geqslant\frac{3^2}{4^3}(1-c)^4M^2N^2$ we obtain $|\mathcal{L}|\geqslant\frac{3^2c(kc-1)}{2^5\times5^2}(1-c)^4NM^3=\Omega(NM^3)$ where each line in $\mathcal{L}$ is $\Theta(\frac{N}{M})$ rich.

The Szemerédi-Trotter bound for point set $\mathcal{P}$ states that the number of $\frac{N}{M}$ rich lines is $O\big(\frac{(N^2)^2}{(N/M)^3}+\frac{N^2}{N/M}\big)=O\big(NM^3\big)$. So we have achieved the Szemerédi-Trotter upper bound for any richness. □

Theorem 12. *For any non-square integer k, any large enough N and $r\leqslant N$, let the point set $\mathcal{P}=A_N^2$ where $A_N=\Big\{x_1+x_2\sqrt{k};x_1,x_2\in\Big[-\sqrt{N},\sqrt{N}\Big]\Big\}$. Then there exists a set of r-rich lines $|\mathcal{L}_r|$ such that*

$$|\mathcal{L}_r|=\Omega\bigg(\frac{|\mathcal{P}|^2}{r^3}+\frac{|\mathcal{P}|}{r}\bigg).$$

4 Applications

In this section we prove Lemma 5 and Corollary 6, two sharp examples of the inverse discrete Loomis-Whitney problem in the plane. We use the family of constructions from Theorem 3 to show two lemmas bounding additive and multiplicative energies [21] are sharp.

Corollary 6.
For any non-square integer k, and large enough N, let the point set $\mathcal{P} = A_N^2$ where $A_N = \left\{x_1 + x_2\sqrt{k}; x_1, x_2 \in \left[-\sqrt{N}, \sqrt{N}\right]\right\}$. Then for any constant $p = O(1)$ there is a set of projections $\left\{\pi_i\right\}_{i=1}^{\Theta(p)}$ such that $|\pi_i(\mathcal{P})| = \Theta\left(\sqrt{p}n\right)$.

Proof. We see $\mathcal{P}$ as embedded in the larger point set $\mathcal{P}' = A_{4N}^2$. Letting $p = M^2$, we construct the set of $\frac{n}{\sqrt{p}}-$rich lines on $\mathcal{P}'$ from the proof of Theorem 3. These belong to $|S|$ many families of parallel lines each of size $\Theta(\sqrt{p}n)$, such that every point in $\mathcal{P}$ is in exactly one line from every family. The size of the slope set is $|S| = \Theta(M^2) = \Theta(p)$. Letting S be the projection directions, the size of each projection is equal to the number of lines in each family $= \Theta(\sqrt{p}n)$. □

Lemma 5.
Let the point set $\mathcal{P}$ be a section of the integer lattice of size $n \times n$. A one-dimensional projection of $\mathcal{P}$ has size $\Theta(n)$ if and only if the slope of the projection direction is an irreducible rational p/q such that $p, q = O(1)$.

Proof. Any line whose slope is non-rational will go through at most a single point, so the projection of the point set along this direction will have maximal size of n^2. So projections of size $O(n)$ can only exist along rational projection directions.

Taking the case where k is a square so the point set is a square lattice, we know from the proof of Corollary 6 that if $p, q = O(1)$ then the projection along the slope p/q has size $\Theta(n)$.

If $p = \omega(1)$, $y = \frac{p}{q} \cdot x \in [0, n] \implies x/q = o(n)$. Similarly, if $q = \omega(1)$, $y = \frac{p}{q} \cdot x \in [0, n] \implies y/q = o(n)$. In either case there are asymptotically less than n points of the lattice on each line of slope $\frac{p}{q}$. So the projection along $\frac{p}{q}$ has size $\omega(n)$.

□

Lemma 8.
For any non-square integer k, and $M \leqslant N$ let $A_N = \left\{x_1 + x_2\sqrt{k}; x_1, x_2 \in \left[-\sqrt{N}, \sqrt{N}\right]\right\}$ and let $X = S \subset \frac{A_N}{A_N}$ be the slope set from Theorem 3. Then $|X| \leqslant |A_N|^2$ and

$$\sum_{x \in X} E^+(A_N, xA_N) = \Theta\left(|A_N|^3 |X|^{1/2}\right).$$

Proof. We consider the dual situation of the proof of Lemma 2.3 [21]. We let the point set be $\mathcal{P} = A_N^2$ and the line set to be as in the construction from Theorem 3. Then $\sum_{x\in X} E^+(A_N, xA_N) = \sum_{x\in X}\sum_y r^2_{A+Bx}(y) = \Theta\big(\sum_{\text{lines}}(\frac{N}{M})^2\big)$ since each line in the construction is $\frac{N}{M}$ rich. Furthermore there are $\Theta(N\cdot M^3)$ lines in the construction so $\sum_{x\in X} E^+(A_N, xA_N) = \Theta(N^3\cdot M)$. Finally $|A_N| = N$ and $|X| = |S| = \Theta(M^2)$ 9 so we have shown $\sum_{x\in X} E^+(A_N, xA_N) = \Theta\big(|A_N|^3|X|^{1/2}\big)$. $\square$

Acknowledgments

The authors are grateful to Lingxian Zhang for interesting conversations. The authors also thank Gabriel Currier and Chi Hoi Yip for helpful suggestions and the reviewers whose careful reading was very helpful in improving and correcting the paper.

Larry Guth received support from the Simons Investigator Award and Olivine Silier was supported by the Caltech Associates SURF Fellowship.

References

[1] David Alonso-Gutiérrez and Silouanos Brazitikos. Reverse Loomis-Whitney inequalities via isotropicity. *Proceedings of the American Mathematical Society*, 149:817–828, 2021.

[2] 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.

[3] Keith M. Ball. Shadows of convex bodies. *Transactions of the American Mathematical Society*, 327:891–901, 1991.

[4] Jonathan Bennett, Anthony P. Carbery, and James Wright. A non-linear generalization of the Loomis-Whitney inequality and applications. *Mathematical Research Letters*, 12:443–457, 2005.

[5] Jonathan Bennett, Anthony P. Carbery, and James Wright. On the multilinear restriction and Kakeya conjectures. *Acta Mathematica*, 196:261–302, 2006.

[6] Béla Bollobás and Andrew Thomason. Projections of bodies and hereditary properties of hypergraphs. *Duke Mathematical Journal*, 59(2):337–357, 1989.

[7] Enrico Bombieri and Jean Bourgain. A problem on sums of two squares. *International Mathematics Research Notices*, 2015(11):3343–3407, 2015.

[8] Jean Bourgain and Ciprian Demeter. New bounds for the discrete Fourier restriction to the sphere in 4d and 5d. *International Mathematics Research Notices*, 2015(11):3150–3184, 2015.

[9] Stefano Campi, Peter Gritzmann, and Paolo Gronchi. On the reverse Loomis-Whitney inequality. *Discrete & Computational Geometry*, 60(1):115–144, 2018.

[10] Artem Chernikov, David Galvin, and Sergei Starchenko. Cutting lemma and Zarankiewicz's problem in distal structures. *Selecta Mathematica*, 26(2):1–27, 2020.

[11] Ernie Croot and Vsevolod F. Lev. Open problems in additive combinatorics. *Additive Combinatorics*, 43:207–233, 2007.

[12] Gabriel Currier. Sharp Szemerédi-Trotter constructions from arbitrary number fields. arXiv:2304.04900, 2023.

[13] Thao Do. Extending Erdő-Beck's theorem to higher dimensions. *Computational Geometry*, 90, 2020.

[14] György Elekes. On linear combinatorics I. Concurrency – an algebraic approach. *Combinatorica*, 17(4):447–458, 1997.

[15] György Elekes. Sums versus products in number theory, algebra and Erdős geometry. *Paul Erdős and his Mathematics II*, 11:241–290, 2001.

[16] James Glaisher. On the sums of the inverse powers of the prime numbers. *The Quarterly Journal of Pure and Applied Mathematics*, 1981.

[17] Mikhael Gromov. Entropy and isoperimetry for linear and non-linear group actions. *Group, Geometry, and Dynamics*, 2:499–593, 2008.

[18] Nets Katz and Joshua Zahl. An improved bound on the Hausdorff dimension of Besicovitch sets in $\mathbb{R}^3$. *Journal of the American Mathematical Society*, 32(1):195–259, 2019.

[19] Lynn H. Loomis and Hassler Whitney. An inequality related to the isoperimetric inequality. *Bulletin of the American Mathematical Society*, 55:961–962, 1949.

[20] Brendan Murphy. Upper and lower bounds for rich lines in grids. *American Journal of Mathematics*, 143, 2021.

[21] Brendan Murphy, Oliver Roche-Newton, and Ilya D. Shkredov. Variations on the sum-product problem. *SIAM Journal on Discrete Mathematics*, 29:514–540, 2013.

[22] Adam Sheffer and Olivine Silier. A structural Szemerdi-Trotter theorem for Cartesian products. *Discrete & Computational Geometry*, 71(2):646–666, 2023.

[23] Noah Singer and Madhu Sudan. Point-hyperplane incidence geometry and the log-rank conjecture. *ACM Transactions on Computation Theory*, 14(2), 2022.

[24] József Solymosi. Dense arrangements are locally very dense. I. *SIAM Journal on Discrete Mathematics*, 20(3):623–627, 2006.

[25] Endre Szemerdi and William T. Trotter. Extremal problems in discrete geometry. *Combinatorica*, 3(3):381–392, 1983.

[26] D. Zagier. Newman's short proof of the prime number theorem. *The American Mathematical Monthly*, 104(8):705–708, 1997.