Additive Combinatorics and Incidence Geometry: The Szemeredi-Trotter Theorem

Vijay Keswani
11799

Supervised by : Dr. Nitin Saxena

November 13, 2014

Abstract

Additive Combinatorics is new discipline in mathematics with connections to additive number theory, fourier analysis, graph theory and probability. The field has numerous applications to various other fields, including Incidence Geometry (which focuses on the properties of lines and points in various geometries in a combinatorial sense). We consider the survey of Additive Combinatorics and its applications to Incidence Geometry by Zeev Dvir [1], and present in particular the Szemeredi-Trotter problem from [1]. The Szemeredi-Trotter theorem basically asks that given a set of points and a set of lines, what is the maximum number of incidences that can exist between the lines and the points? We consider the cases of finite fields and reals and examine the upper bounds on the number of incidences in both settings.

This project was done in conjuction with Anurag Sahay, a fourth year undergraduate in the Dept. of Computer Science and Engineering, who read on the Kakeya Problem, which deals with the notion of “size” of a subset of $\mathbb{R}^n$ or of $\mathbb{F}^n$ which has a “line” in every “direction”. at the same time as when I was reading on the Szemeredi-Trotter Theorem, and both of us attended each others project presentations. The presentations were also attended by Dr. Nitin Saxena and Dr. Rajat Mittal from the Dept. of Computer Science and Engineering. Throughout this report, we follow [1], except where we note otherwise.

This report was submitted as part of the course CS498A (Undergraduate Project) done in the 2014-15/1st Semester, under the supervision of Dr. Nitin Saxena.

Contents

1 Introduction and Preliminaries **5**

1.1 Additive Combinatorics 5

1.2 Rusza Calculus 8

1.3 Szemeredi-Trotter Problem 10

2 Counting Incidences over Finite Fields **11**

2.1 Trivial Upper bound using Cauchy-Swartz inequality 11

2.2 Balog-Szemeredi-Gowers Theorem 12

2.2.1 Additive Energy 13

2.2.2 Proof of BSG Theorem 14

2.3 Growth in $\mathbb{F}_p$ 16

2.4 Szemeredi-Trotter theorem for finite fields 16

2.4.1 Translating the problem to a grid 17

2.4.2 Projective space $\mathbb{PF}^n$ 19

2.4.3 Solving the problem on a grid 20

2.5 Sum-Product Estimate in Finite Fields 22

3 Counting Incidences over Reals **24**

3.1 Crossing Number Inequality 24

3.2 Proof of Szemeredi-Trotter Theorem in Reals 26

Notation

Throughout this report, we use the notation

$$f \lesssim g \text{ [and correspondingly, } f \gtrsim g]$$

to mean that there exists a positive constant C such that

$$f \leq Cg$$

The implicit constant C may depend on some quantities (say ϵ, δ etc.). In this case, the quantities may be specified either in writing or as a subscript (say $\ll_\epsilon$ or $\mathcal{O}_\delta$).

We also use the somewhat non-standard notation

$$f \sim g$$

to denote both $f \lesssim g$ and $f \gtrsim g$ occurring simultaneously.

We will use $\mathbb{F}$ exclusively to denote a finite field with cardinality q.

We use the indicator notation

$$1_P = \begin{cases} 1 & \text{if } P \text{ holds} \\ 0 & \text{if } P \text{ does not hold} \end{cases}$$

1 Introduction and Preliminaries

In this reading project, we considered the fields of Additive Combinatorics and Incidence Geometry. In particular, we looked at the Szemeredi-Trotter problem in both the reals as well as the finite fields. In this report, we record mostly the material by me during project presentations, starting with a basic introduction to Additive Combinatorics (we will quote a few results without proof). We then move on to an introduction to the Szemeredi-Trotter theorem, and treat the problem first in the finite field case, and then in the reals case, in both cases proving as much as was done in [1].

We will assume basic familiarity with group theory, finite fields, real projective spaces, affine spaces and real numbers. We will also assume some familiarity with using the Cauchy-Schwarz inequality, even though we will explicitly mention whenever we use it in our proofs.

In the paper, we have tried to give an intuitive and informal proof of every statement which needs a proof. For the more important theorems, a formal proof is also given, while for the rest, a proper reference has been cited.

I would like to thank Anurag Sahay for his contributions to this report, as the sections on introduction to Additive Combinatorics and a brief overview of projective spaces has been prominently written by him.

1.1 Additive Combinatorics

The field of Additive Combinatorics is a relatively new field which is connected to, and uses ideas from additive number theory, group theory, graph theory and probability. We refer the reader to [2] for an overview of Additive Combinatorics with a specific view towards Computer Science.

In the general setting of Additive Combinatorics, one studies the combinatorial properties of some commutative group G. In particular, suppose $(G, +)$ is the group written in additive notation, and suppose $A, B \subset G$ are arbitrary subsets, then we define the sumset $A + B$ as follows:

$$A + B := \{a + b : a \in A, b \in B\}$$

Note that for a commutative group, this is a commutative set operation. Furthermore, it is an associative set operation.

We can define the difference set $A - B$ in a similar manner (where $a - b = a + (-b)$ and $-b$ is the additive inverse of b in G). We will also use $2A$ to denote $A + A$, $3A$ to denote $A + A + A$ and so on. We will also define the k-dilate as follows:

$$k \cdot A = \{ka : a \in A\}$$

Sometimes we may abuse notation and use kA where we actually mean $k \cdot A$ assuming that the situation is clear from the context. We will also abuse notation to denote the set $\{a\} + A$ as $a + A$.

For typical applications, G will either be the reals or the finite fields, or related groups such as integers, rationals etc. Furthermore, most theorems and applications deal specifically with the case where A and B are finite. We are then interested in the cardinality of the sets and sumsets, and the relationship between them.

In particular, we have the following basic inequality:

Theorem 1.1 (Basic Sumset Inequality)**.** *For the real numbers $\mathbb{R}$, and finite subsets $A, B \subset \mathbb{R}$, we have the following inequality:*

$$|A| + |B| - 1 \leq |A + B| \leq |A||B|$$

further, equality may occur on both sides. Further, if $\mathbb{R}$ is replaced by any arbitrary group, the upper bound still holds.

Proof. The upper bound is trivial. To see this, note that the map $(a, b) \mapsto a + b$ is a map from $A \times B$ to G whose image is exactly $A + B$. Since this map is surjective on $A + B$, we get that

$$|A + B| \leq |A \times B| = |A||B|$$

Further, for $\mathbb{R}$ let $r = |A|$, $s = |B|$ and let $A = \{a_1, \cdots, a_r\}$ and $B = \{b_1, \cdots, b_s\}$. Further, arrange the indices in a manner so that

$$a_1 > a_2 > \cdots > a_r$$

and

$$b_1 > b_2 > \cdots > b_s$$

We thus have that

$$a_1 + b_1 > a_2 + b_1 > \cdots > a_r + b_1$$

and we have

$$a_r + b_1 > a_r + b_2 > \cdots > a_r + b_s$$

and thus, the sequence $a_1+b_1, a_2+b_1, \cdots, a_r+b_1, a_r+b_2, \cdots, a_r+b_s$ consists of $r + s - 1$ distinct elements in $A + B$. Thus, we have that

$$|A+B| \geq \#\{a_1+b_1, a_2+b_1, \cdots, a_r+b_1, a_r+b_2, \cdots, a_r+b_s\} = |A|+|B|-1$$

This gives the inequality. To see that both equalities can occur, take the case where A and B are arithmetic progressions with the same common difference, and the case where $A = \{0, 1, 2, 3, \cdots n\}$ and $B = \{0, n+1, 2n+2, 3n+3, \cdots mn+m\}$.

□

The basic upper bound denoted above is weak but pretty useful in many circumstances.

The properties of subsets under this set operation are very useful in characterizing "structure" in the subsets. For example, if A is a subgroup, we automatically have that $A + A = A$, and thus $|2| = |A|$. In fact, $|2A| = |A|$ implies that A is either a group or a coset of a group. To see this, note that we can assume without loss of generality that $0 \in A$, for if this is not so, we can replace A with $A - a$ for some $a \in A$. Hence, $A = 0 + A \subset A + A = 2A$. Further, $|2A| = |A|$. Hence, we must have $2A = A$, and thus we have that A is finite close subset of G, and hence a closed subgroup of G.

The basic theory of set addition is known by the name of Rusza Calculus. We will now present some basic Rusza Calculus.

1.2 Rusza Calculus

The fundamental result in Rusza Calculus is the triangle inequality, viz.

Theorem 1.2 (Rusza triangle inequality)**.** *Let G be an abelian group, and $A, B, C \subset G$. Then we have the following inequality among cardinalities:*

$$|A||B - C| \leq |A + B||A + C|$$

Proof. For any $x \in B - C$, fix a representation $x = b - c = b(x) - c(x)$ with $b \in B$ and $c \in C$. Now define a map $f : A \times (B - C) \to (A + B) \times (A + C)$ as $f(a, x) = (a + b, a + c)$.

Now, suppose $f(a, x) = f(a', x')$. Thus, $x = b - c = (a + b) - (a + c) = (a' + b') - (a' + c') = b' - c' = x'$. Since we fixed a representation, this implies that $b = b'$ and $c = c'$, and hence $a = a'$.

Thus, f is an injective map. Comparing the cardinalities of the domain and co-domain, the theorem follows.

□

To see why this theorem is called a triangle inequality, we first define the following notion of distance between subsets of a group:

Definition 1.1 (Rusza distance)**.** The *Rusza distance* $d(A, B)$ between two sets $A, B \subset G$ is defined as

$$d(A, B) = \log \frac{|A - B|}{|A|^{1/2}|B|^{1/2}}$$

It is easy to see that this distance is symmetric since $|A - B| = |B - A|$. Further, note that the triangle inequality

$$d(A, C) \leq d(A, B) + d(B, C)$$

can be rewritten, by taking exponentials both sides to

$$\frac{|A - C|}{|A|^{1/2}|C|^{1/2}} \leq \frac{|A - B|}{|A|^{1/2}|B|^{1/2}} \times \frac{|B - C|}{|B|^{1/2}|C|^{1/2}}$$

or, in other words,

$$|A - C||B| \leq |A - B||B - C|$$

This is equivalent to the previous theorem (which can be seen by replacing (A, B, C) in the previous theorem by $(-B, A, C)$).

Thus, the previous theorem is actually equivalent to the statement that the Rusza distance defined above satisfies the triangle inequality.

The Rusza disance is, however, clearly not reflexive in the general case.

The Rusza distance is a very useful tool for proving general inequalities. In particular, it allows us to connect the notion of sets that grow slowly under addition and substraction. For example, we have the following theorem:

Theorem 1.3. *If* $|A + A| \leq K|A|$ *for some absolute constant* K*, then we have* $|A - A| \leq K^2|A|$*. Conversely,* $|A - A| \leq K|A|$ *implies* $|A + A| \leq K^2|A|$*.*

Proof. Note that

$$\frac{|A - A|}{|A|} = \exp(d(A, A)) \leq \exp(d(A, -A) + d(-A, A)) = \frac{|A + A|^2}{|A|^2}$$

and that

$$\frac{|A + A|}{|A|} = \exp(d(A, -A)) \leq \exp(d(A, A) + d(-A, -A)) = \frac{|A - A|^2}{|A|^2}$$

Both these inequalities together with the respective hypothesis give the desired conclusion.

□

For a given K, a set satisfying $|A + A| \leq K|A|$ is said to be a set of small doubling. The expectation is that if A has small doubling, then in fact, all possible additions and substractions of A with itself must be small (since there must be inherent structure in A of some sort). The formal result is by Plünneke and Rusza:

Theorem 1.4 (Plünneke-Rusza inequality, $\star$)**.** *Let G be an abelian group, and $A, B \subset G$ be sets of equal size satisfying $|A+B| \leq K|A|$. Then we have*

$$|kA - lA| \leq K^{k+l}|A|$$

We now move on to an introduction to the Szemeredi-Trotter problem.

1.3 Szemeredi-Trotter Problem

Consider a set of points P, in some vector space, and a set of lines L; an incidence is a pair $(p, l) \in P$ x L, such that point p lies on line l. The Szemeredi-Trotter theorem gives an upper bound on the number of such incidences.

In case of reals, there is a tight upper bound on the number of incidences. It has been shown to be $\mathcal{O}((|P||L|)^{2/3} + |P| + |L|)$ [7]. A detailed proof of this has been given in Section 3.

In the case of finite fields, much less is known about the upper bound on the number of intersections between N points and N lines in the field. If nothing is assumed on the field, the best upper bound we get is $\sim N^{1.5}$, which we get from a simple Cauchy-Swartz calculation.

However we obtain a small improvement of the form $N^{1.5-\epsilon}$, where $\epsilon > 0$, for the finite field, say $\mathbb{F}_q$ which does not contain large subsets and if we bound $N \ll q^2$. This was shown by Bourgain, Katz and Tao [3], as an application of the sum-product theorem over finite fields. The reason why this better bound is relevant is because, it was shown by the same authors [3], that there is a direct co-relation between the upper bound on the number of incidences in finite fields and the sum-product estimate for the finite fields. Hence any improved bound here would give a better sum-product estimate and vice-versa.

In the sections below, we first discuss in detail the trivial upper bound of $N^{1.5}$ and the improved upper bound of $N^{1.5-\epsilon}$ for the number of incidences in finite fields. However, before jumping to the proof of the improved upper bound, we develop a few set of tools, mainly from Additive Combnatorics, which will be useful to us later, when studying the proof of Szemeredi-Trotter.

One of the tools that we use is the Balog-Szemeredi-Gowers theorem [henceforth referred to as BSG theorem], which talks about the conditions under which large subsets of given sets do not grow under addition. The BSG theorem has been used in various other important results in different fields of Additive Combinatorics [including Szemeredi Theorem, which talks about arithmetic progressions of different sizes in large sets], and plays a crucial role in our proof as well.
Also, before ending this section, for the sake of completeness, we briefly discuss the relation of this problem with the sum-product estimate, which we consider relevant to this survey.

We then move on to the case of counting incidences in reals and discuss the proof for the tighter upper bound that we have in this case.

2 Counting Incidences over Finite Fields

This section covers the proof of Szemeredi-Trotter theorem for the finite field case. The proof will mostly follow the outline provided in survey [1], along with certain references from [3].

We will first prove the trivial upper bound for the number of incidences in a general vector space.

2.1 Trivial Upper bound using Cauchy-Swartz inequality

Definition 2.1 (Set of incidences)**.** Let P be a set of points and L be a set of lines in a vector space, then define the set $I(P, L)$ as :

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

Claim 2.1. *Given a set P of N points and a set L of N, $|I(P, L)| \leq N^{1.5}$*

Proof. For each $l \in L$, we define $P(l) = \{p | p \in P \text{ and } p \in l\}$.

Observe that $|I(P, L)| = \sum_{l \in L} P(l)$

$$|I(P, L)|^2 = (\sum_{l \in L} P(l))^2$$

Applying Cauchy-Swartz inequality, we get

$$|I(P,L)|^2 \leq N \sum_{l \in L} P(l)^2$$

The right hand side represents number of ways choosing two points [repitition allowed] that lie on the same line. Since two distinct points can determine atmost one line, we can see that

$$\sum_{l \in L} P(l)^2 \leq |P|^2 + |I(P,L)|$$

Hence, we get

$$|I(P,L)|^2 \leq N^3 + N.|I(P,L)|$$

From the above quadratic inequality we can easily derive that $|I(P,L)| \leq N^{1.5}$ □

Before we move to the main proof, we will derive certain Additive Combinatorics results, to help us with the proof. First we state and partially prove the Balog-Szemeredi-Gowers Theorem, which talks about large subsets which do not grow under addition. The original theorem was given and proved by Balog and Szemeredi [4], and an improved bound for the same by Gowers [5], which is used here.

2.2 Balog-Szemeredi-Gowers Theorem

Let G be an abelian group and $A, B \subset G$ be subsets. We use the notion of sumset $A + B$ (and correspondingly difference set), as defined in Section 1.1.

Further we also define $Q(A,B)$ and $E(A,B)$, for the above sets A and B as follows :

Definition 2.2. $Q(A,B) = \{(a,a',b,b') \in A \times A \times B \times B | a + b = a' + b'\}$

Definition 2.3 (Additive Energy of $A + B$)**.**

$$E(A,B) = \frac{|A|^2|B|^2}{|Q(A,B)|}$$

The statement of the BSG theorem is as follows :

Theorem 2.1 (BSG Theorem [5]). *Let $A, B \subset G$ be sets of size N in an abelian group G. Suppose that $E(A, B) \leq KN$. Then, there exists subsets $A' \subset A$ and $B' \subset B$ with $|A'|, |B'| \geq N/K^c$ such that $|A' + B'| \leq K^c N$. Here, $c > 0$ is an absolute constant.*

2.2.1 Additive Energy

As a small aside, we will disuss briefly about the Additive energy of two sets defined above and why it is relevant in our discussion.

From the above definition, it can be easily seen that

$$max|A|, |B| \leq E(A, B) \leq |A + B|$$

To get an intuitive idea about $E(A, B)$, let us consider a few examples. If A is an arithmetic progression of size N, then it is easy to see that $|A+B| \lesssim N$, since sum of most elements will give an element of the set itself.
Also observe that $|Q(A, A)| \sim N^3$, since choosing any 3 elements of set A will uniquely identify the fourth, hence $E(A, A)$ will also be bounded by N.

Now consider a set B of size N with no dependencies amongst the elements. For this set,

$$|B + B| = \frac{1}{2}|B|(|B| - 1)$$

Also if there are no dependencies, $Q(B, B)$ will consists of quadruples (a, a', b, b') such that $a = a'$ and $b = b'$, therefore $|Q(B, B)|$ will be N^2 and correspondingly $E(B, B) = N^2$.

However, taking $C = A \cup B$, since $|C + C| \gtrsim |B|^2$, we get that

$$|C + C| \gtrsim |C|^2$$

but because $|Q(C, C)| \geq |Q(A, A)|$, we also have

$$E(C, C) \lesssim |C|$$

Hence using $E(C, C)$, we can infer that even though the set C grows under addition with itself, there exists a large enough subset of C (in this case A) which does not grow much under addition.

The BSG theorem, in its essence, tries to formalise and generalise this intuitive notion.

2.2.2 Proof of BSG Theorem

The BSG theorem can be proved using the following generic graph theoretic lemma :

Lemma 2.1. *Let $H \subset V \times U$ be a bipartite graph with $|V| = |U| = N$. Suppose $|H| \geq \alpha N^2$ denote the number of edges. Then, $\exists\ V' \subset V$ and $U' \subset U$ with $|V'|, |U'| \geq \alpha^c N$ and such that $\forall\ v \in V', u \in U'$, there are atleast $\alpha^c N^2$ paths of length three between v and u.*

First we see how this lemma implies the BSG theorem and then we give an informal proof of lemma.

Proof of BSG Theorem. Suppose for the given sets $A, B \subset G$, we have $E(A, B) \leq KN$. Then, $|Q(A, B)| \geq N^3/K$.
For a particular x, define $R(x)$ as

$$R(x) = (a, b) \in A \times B | a - b = x$$

Further define set $P = \{x|\ |R(x)| \geq N/2K\}$. Each element of P is called a *popular difference.* We can show that $|P| \geq N/2K$.

We construct the graph using these sets A and B, taking the elements of the sets to be the vertices and drawing edges between (a, b) if $a - b \in P$. For this graph, let E denote the set of edges. Then,

$$|E| \geq |P|.N/2K$$

$$\implies |E| \geq N^2/4K^2$$

Hence, we can apply Lemma 2.1 on this graph, with $\alpha = (1/4K^2)$.
From the lemma, we can infer that there exists $A' \subset A$ and $B' \subset B$ with $|A'|, |B'| \geq N/K^c$, such that $\forall\ a \in A', b \in B'$, there are atleast $\alpha^c N^2$ paths of length three between a and b.

Consider one such path from a to b. Let this path be consist of vertices a, b', a', b. We can write $a - b = a - b' + b' - a' + a' - b$

$$\implies a - b = a - b' - (a' - b') + a' - b$$

$$\implies a - b = x_1 - x_2 + x_3$$

where x_1, x_2, x_3 are all popular differences.

Since there are $\alpha^c N^2$ such paths of length three between each pair a and b, each difference $a - b$ can be expressed using $\alpha^c N^2$ such triplets of popular differences.
Therefore, if we look to express all such differences in $A - B$ using these triplets, we can see that

$$|A - B| \leq \frac{|P|^3}{\alpha^c N^2}$$

$$|A - B| \leq N.(4K^2)^c$$

$$|A - B| \leq K^{c'} N$$

Using Theorem 1.3, we can see that this implies $|A + B| \leq K^{c''} N$ □

Hence we can see that if Lemma 2.1 is true, then BSG Theorem follows.

We now give an intuition into why Lemma 2.1 will be true. The proof for the lemma follows an expectation argument. We first try to check for existence of many paths of length two with a subset of vertices. Note that this a simpler statement than Lemma 2.1.

The main idea of the proof [courtesy of Gowers] is that if we choose a random vertex $u \in U$, then for the set of neighbours of u in V, (say V'), the number of paths of length two for most pairs in $V \times V$ will be atleast $\epsilon|V|^2$. Intuitively, this can be seen to be true because the set we are taking already has a lot of paths of length two. The notion is quantified using an expection argument in the proof.

Next, once we have proved that there are a lot of paths of length two in a subset of V, we find a subset of U which has a lot of neighbours in V. Once again we use an expectation argument to prove the existence of such a subset. Then using these subsets of U and V, we start constructing the paths of length three and the theorem follows from it.

To study the formal proof of BSG theorem, we refer the reader to the original papers on the topic by Balog-Szemeredi [4] and the improvement given by Gowers [5].

A corollary of the BSG theorem is :

Corollary 2.1 ([10])**.** *Let $A \subset \mathbb{F}_{|}$ and $T \subset \mathbb{F}_{|}{}^*$. Suppose that for all $\lambda \in T$, we have $E(A, \lambda A) \leq K|A|$. Then there exists $A' \subset A$ and $T' \subset xT$ (for some $xin\mathbb{F}^*$), such that $|A'| \geq |A|/K^c$, $|A'| \geq |A|/K^c$ and with $|A' + \lambda A'| \leq K^c|A'|$, for all $\lambda \in T'$.*

2.3 Growth in $\mathbb{F}_p$

In this section, we look at the properties of a set under addition, specifically the size of the sumset. We consider the field F_p, since it does not contain any subfield [required in the proof], however it can be extended to any field which does not contain large subfields. We denote $\lambda A = \{\lambda.a | a \in A\}$.

Our goal is to show that for some $\lambda \in \mathbb{F}$, $|A + \lambda A| \gg |A|$.

Theorem 2.2. *Let $A, T \subset \mathbb{F}_p$ with $p^\alpha \leq |A| \leq p^{1-\alpha}$ and $|T| \geq p^\beta$. Then there exists $\lambda \in T$, such that $|A + \lambda A| \geq |A|^{1+c(\alpha,\beta)}$, where c is a constant depending only on α and β.*

We omit the proof of the above theorem and refer the curious readers to the survey [1] for the detailed proof. However we will discuss the consequences of the theorem.

Theorem 2.2 and Corollary 2.1 together imply the following energy version of Theorem 2.1.

Theorem 2.3. *Let $A, T \subset \mathbb{F}_p$ with $p^\alpha \leq |A| \leq p^{1-\alpha}$ and $|T| \geq p^\beta$. Then there exists $\lambda \in T$, such that $E(A, \lambda A) \geq |A|^{1+c(\alpha,\beta)}$, where c is a constant depending only on α and β.*

The above theorem will be used in the proof of Szemeredi-Trotter theorem, where it will play an important role.

2.4 Szemeredi-Trotter theorem for finite fields

We are now ready to prove the Szemeredi Trotter theorem to get a bound on the number of incidences of N points and N lines in $\mathbb{F}_p^2$.

Theorem 2.4 (ST theorem over finite fields [1])**.** *Let L be the set of N lines in $\mathbb{F}_p^2$ and let P be the set of N points in $\mathbb{F}_p^2$. Then if $p^\alpha < N < p^{1-\alpha}$ for some $\alpha > 0$, then $|I(P, L)| \lesssim N^{1.5-\epsilon}$, where ϵ depends only on α.*

The proof of the ST theorem is divided into two parts :

1. Reducing the problem space to a grid.
2. Solving the problem over a grid.

The intuitive way to consider this proof is that we are analysing the cases in which the number of incidences might be high. We proceed by finding certain regularity conditions under which we would expect the bound of $N^{1.5-\epsilon}$ to be violated. To be more precise, if we assume that the number of incidences are very close to $N^{1.5}$, then this would force most of the N points to lie on a $N^{0.5} \times N^{0.5}$ grid and then we can prove our contradiction.

We use the following notations in our proof : For a line $l \in L$,

$$P(l) = \{p \in P | p \in l\}$$

For a point $p \in P$,

$$L(p) = \{l \in L | p \in l\}$$

The proof the ST theorem is by contradiction. That is, suppose that $|I(P, L)| \gg N^{1.5-\epsilon}$. We will show that we can choose $\epsilon > 0$ such that we arrive at a contradiction. Note that we still have an upper bound of $N^{1.5}$, that we derived earlier using Cauchy-Swartz inequality. Hence by our assumption we have,

$$N^{1.5-\epsilon} \ll |I(P, L)| \leq N^{1.5}$$

We start with removing certain lines and points, such that our assumption is not affected. Firstly, remove all points which are incident on atmost $N^{0.5-2\epsilon}$. We can see that this would affect our lower bound since, if it did affect our lower bound then the total number of incidences would be $\lesssim N^{1.5-2\epsilon}$.

Next we remove all points $p \in P$ for which $L(p) \gtrsim N^{0.5+2\epsilon}$. Seeing how this does not affect our assumption is slightly non-trivial, but can be inferred using the upper bound of $N^{1.5}$ that we have on the number of incidences. After this step, we will have atleast $N^{1-2\epsilon}$ points remaining, and considering the above lower bound on $L(p)$, the number of incidences will still be $\gtrsim N^{1.5-4\epsilon}$. Hence, in a bad case we might still have the number of incidences to be pretty high. However, we now change our assumption to suit the new setting. Hence, for the assumption $N^{1.5-4\epsilon} \lesssim |I(P, L)| \leq N^{1.5}$, we have for all points $p \in P$,

$$N^{0.5-2\epsilon} \lesssim L(p) \lesssim N^{0.5+2\epsilon}$$

2.4.1 Translating the problem to a grid

To translate this problem to a grid, we find two points $p_0, p_1 \in P$, such that most incidences happens on intersections of lines through p_0 and p_1. Again to see such p_0, p_1 should exist, we see that by our earlier regularity conditions we had a good lower bound on the number of points on each line. Hence if we consider the number of incidences captured by two appropriate sets of lines, we can hope to capture most of the incidences. We formally prove the existence of such p_0, p_1 below.

Claim 2.2. *There exist points $p_0, p_1 \in P$, such that there exists a subset $P' \subset P$ with $|P'| \geq N^{1-c\epsilon}$ and s.t. $P' \subset \{l_0 \cap l_1 | l_0 \in L(p_0), l_1 \in L(p_1)\}$, for some absolute constant $c > 0$.*

Proof. For $p \in P$, define $T(p)$ to be the set of points that lie on some line through p, that is, $T(p) = \{p' \in P | \exists l \in L \text{ s.t } p, p' \in l\}$.

We look at the expected value of $|T(p_0) \cap T(p_1)|$ to see if it satisfies the above claim.

$$\mathbb{E}[|T(p_0) \cap T(p_1)|] = \frac{1}{N^2} \sum_{p_0, p_1 \in P} \sum_{q \in P} \sum_{l_0, l_1 \in L(q)} 1_{p_0 \in l_0} . 1_{p_1 \in l_1}$$

$$= \frac{1}{N^2} \sum_{q \in P} (\sum_{l \in L(q)} |P(l)|)^2$$

Applying Cauchy-Swartz,

$$\mathbb{E}[|T(p_0) \cap T(p_1)|] \geq \frac{1}{N^3} (\sum_{q \in P} \sum_{l \in L(q)} |P(l)|)^2$$

$$= \frac{1}{N^3} (\sum_{l \in L} |P(l)|^2)^2$$

Again applying Cauchy-Swartz,

$$\mathbb{E}[|T(p_0) \cap T(p_1)|] \geq \frac{1}{N^5} (\sum_{l \in L} |P(l)|)^4$$

$$\geq \frac{1}{N^5} (N^{1.5-4\epsilon})^4 \geq N^{1-c\epsilon}$$

Hence we have proved that such p_0, p_1 exist, and we can then take our required set $P' = T(p_0) \cap T(p_1)$. □

Now if we replace P by P', the number of incidences are $\gtrsim N^{1.5-c\epsilon}$ (using the lower bound on $L(p)$) and we can again argue that we might still have a configuration which satisfies our incidence assumptions. Hence we take this "bad case" and analyse this further by converting it into a grid. Note however that in our new setting we change our assumption to be $N^{1.5-c\epsilon} \lesssim |I(P,L)| \leq N^{1.5}$.

To translate this problem to a grid, we embed our space into the projective space $\mathbb{PF}^2$ and take linear transformation to send p_0 and p_1 to the line at infinity.

2.4.2 Projective space $\mathbb{PF}^n$

We take a small detour from our discussion to briefly introduce the concept of projective spaces over finite fields and later in this section also show the reduction of our setting to a grid.

The projective space over a finite field $\mathbb{F}$ is defined pretty similarly to projective spaces over the real numbers $\mathbb{R}$ the n-dimensional projective space is essentially the set of all directions in the $n+1$-dimensional linear space over $\mathbb{F}$. More formally, it is the space obtained by collapsing all points lying on lines passing through the origin into each other. That is,

Definition 2.4 (Projective Space over $\mathbb{F}$)**.** Let $\mathbb{F}^{n+1}$ be the $n+1$ dimensional linear space over $\mathbb{F}$. We define the equivalence relation $\sim_P$ for $x, y \in bF^{n+1} - \{0\}$ as follows:

$x \sim_P y$ if and only if there exists a non-zero $\lambda \in \mathbb{F}^*$ such that $x = \lambda y$. We call the resulting quotient space under this relation as the *projective space of dimension n over* $\mathbb{F}$, denoted as $\mathbb{PF}^n$.

We will call the process of taking the equivalence relations *projectivizing.* Furthermore, all linear maps from $\mathbb{F}^{n+1}$ that remain well-defined after projectivization shall be known as projective maps from $\mathbb{PF}^n$.

Points in $\mathbb{PF}^n$ shall be denoted by the $n+1$ homogenous coordinates (which are unique up to multiplication by a non-zero scalar) $x = (x_0 : x_1 \cdots : x_n)$.

Now note that the n-dimensional affine space $\mathbb{F}^n$ can be embedded into $\mathbb{PF}^n$ by mapping the point $(x_1, \cdots, x_n) \in \mathbb{F}^n$ to $(1 : x_1 : \cdots : x_n) \in \mathbb{PF}^n$, and this map will respect the structure (whereby projective maps will reduce to affine maps for the embedded affine space). Once this embedding has been fixed, the points in $\mathbb{PF}^n$ having $x_0 = 0$, that is, points of the form $(0 : x_1 : \cdots : x_n)$ are known as the *points at infinity.* The set of all these points is then known as the hyperplane at infinity, analogous to real projective case.

Now consider any line l in $\mathbb{F}^n$ say

$$a_0 + a_1x_1 + a_2x_2 + \cdots + a_nx_n = 0$$

It is easy to see that after projectivizing, $x_0 = 1$, so by homogenizing the line will now become

$$a_0x_0 + a_1x_1 + \cdots + a_nx_n = 0$$

This "line" is now completed to include points with $x_0 = 0$. It is easy to see that affine points on this completed line are the same as those on the unprojectivized line.

Consider a line in l in $\mathbb{F}^2$, given by the equation $ax + by + c = 0$. When this space is embedded in $\mathbb{PF}^2$, a point (x, y) in $\mathbb{F}^2$, which lies on line l, will be represented by $(1, x, y)$ in $\mathbb{PF}^2$ and will satisfy the equation $ax+by+cw = 0$. The point of infinity for this line will be given by the homogenous co-ordinate $(-b, a, 0)$. Observe that the point of infinity is uniquely determined by the direction of the corresponding line in $\mathbb{PF}^2$. Hence all lines having the same point at infinity when embedded in $\mathbb{PF}^2$, have the same direction in $\mathbb{PF}^2$.

We go back to out setting of points P' and lines L. We embed these into $\mathbb{PF}^2$ and take a linear transformation to send p_0 to (0,1,0) and p_1 to (1,0,0). Hence in $\mathbb{PF}^2$, all lines passing through p_0 will now be parallel to the X-axis and all lines passing through p_1 will be parallel to the Y-axis. We can now remove the $w = 1$ homogenous part of the co-ordinate and go back to solving our for a grid in $\mathbb{F}^2$ represented by $A \times B$. Note that since there can be atmost $L(p_0)$ or $L(p_1)$ number of parallel lines, we have that $|A|, |B| \lesssim N^{0.5+2\epsilon}$, by our earlier bound on $L(p)$.

2.4.3 Solving the problem on a grid

Claim 2.3. *Let P,L denote set of atmost N points and lines and* $P \subset A \times B$ *with* $|A|, |B| \leq N^{0.5+2\epsilon}$. *If* $p^\alpha < N < p^{2-\alpha}$ *for small* $\alpha > 0$, *then* $|I(P, L)| \leq N^{1.5-c\epsilon}$.

Proof. We first give a few definitions before going into the proof. The set $R(b)$ denotes the points in P with Y-coordinate as b, for each $b \in B$. Also, $H(b)$ denotes set of lines that passes through some point in $R(b)$. Observe that if we remove all those lines which have atmost $N^{0.5-2\epsilon}$ points on them, we do not affect the number of incidences by any significant amount, considering our assumption on them. Hence we have that $P(l) \geq N^{0.5-2\epsilon}$ for all $l \in L$

Similar to our previous argument, we claim that there exists b_0 and b_1, such that $H(b_0)$ and $H(b_1)$ contains many lines. To see this we look at the expected value of $|H(b_0) \cap H(b_1)|$ and find it to be greater than $N^{1-c\epsilon}$ [the exact calculation can be easily done using Cauchy-Swartz inequality and the fact that each line can intersect $R(b)$ in atmost one point].

W.l.o.g, consider (b_0, b_1) to be (0,1). Denote L' to be $H(b_0) \cap H(b_1)$. Then considering our lower bound on $P(l)$, we have that $|I(P, L')| \gtrsim N^{1.5-c\epsilon}$.

Since points in $R(0)$ and $R(1)$ can constitute atmost $\mathcal{O}(N)$ incidences, most of the incidences lie on points with $b \neq 0, 1$, i.e.,

$$|\{(p, l) \in P \times L' | p \in l \text{ and } p \notin R(0) \cup R(1)\} \gtrsim N^{1.5-c\epsilon}$$

If we consider any line $l \in L'$, we can say that it passes through three points $(x_0, 0)$, $(x_1, 1)$ and a general point (a, b). Then these three points should satisfy the equation

$$a = x_0 + (x_1 - x_0)b$$
$$\implies a = bx_1 + (1-b)x_0$$

Hence we can alternately write the above set (and hence bound it) as

$$|\{(b, x_0, x_1) \in B \times A \times A | bx_1 + (1-b)x_0 \in A\} \gtrsim N^{1.5-c\epsilon}$$

This implies that there exists $B' \subset B$ with $|B'| > N^{0.5-2c\epsilon}$, such that for all $b \in B'$

$$|\{(x_0, x_1) \in A \times A | bx_1 + (1-b)x_0 \in A\} \gtrsim N^{1-2c\epsilon}$$

Informally the above bound says that there exists a large enough subset of A which does not grow under addition. Formally, we can see that if we divide the above expression by b and then use the upper bound on additive energy of two sets $E(A, B) \leq |A + B|$, we get that

$$E(A, \frac{b}{1-b}A) \leq N^{0.5+\mathcal{O}(\epsilon)} = |A|^{0.5+\mathcal{O}(\epsilon)}$$

If we take $p^\alpha < N < p^{2-\alpha}$ and ϵ to be small enough, we contradict Theorem 2.3. This completes the proof of ST theorem for finite fields.

□

2.5 Sum-Product Estimate in Finite Fields

For a non-empty subset A of a finite field, we had earlier defined the notion of sumset $A + A$. Similarly, we define the notion of product set as

$$A.A = \{a.b|a, b \in A\}$$

Clearly, we have the bound

$$|A + A|, |A.A| \geq |A|$$

In case A is a subfield, it can be seen that the bound will be sharp. However if we know that A is not a subfield, then we can hope to improve this lower bound for the size of sumset or product set. Hence to ensure A is not a subfield, we take F to be a prime field $\mathbb{F}_{|}$.

Formally the sum-product theorem in finite fields can be stated as follows :

Theorem 2.5 (Sum-Product Estimate [3]). *Let $F = \mathbb{F}_{|}$ for some prime p, and let $A \subset F$ with*

$$|F|^\delta < |A| < |F|^{1-\delta}$$

for some $\delta > 0$. Then one has a bound of the form

$$max(|A + A|, |A.A|) \geq c(\delta)|A|^{1+\epsilon}$$

for some $\epsilon = \epsilon(\delta) > 0$

To make the sum-product theorem clear, let us take an example. Consider A to an arithmetic progression. In that case $A+A$ will mostly contain terms of A itself, and so $|A + A| \leq c|A|$, for some small constant c, while $A.A$ can be seen to contain $|A|$ APs in itself and so will have size $\sim |A|^2$.

However if we consider A to a geometric progression, we observe the exact opposite thing. In this case $|A + A| \sim |A|^2$, because elements of GP are additively not corelated, while $|A.A| \leq c|A|$, for some small constant c.

Hence the sum-product theorem, in a sense, can be seen to state that a set cannot behave like a arithmetic progression and a geometric progression simultaneously.

Similar to the problem of Szemeredi-Trotter theorem ,the value of ϵ in the theorem is not known. An integer analogue of the theorem was given by Szemeredi and Erdos [9] and after many improvements, the best bound for the integer analogue is known to be $\epsilon = 1/4$, obtained by Elekes [6].

The interesting aspect for us to note is that, the connection between incidence problems and sum-product estimate in finite field is much deeper. The same has been explored recently by Bourgain, Katz and Tao in their paper "A sum-product estimate in finite fields, and applications". The paper proved the sum-product bound and also gave the applications to incidence theorems. This project and the report has been heavily influenced by this paper.

Before this paper, Elekes [6] had proved a connection between the Szemeredi-Trotter problem in finite fields and the sum-product problem :

Theorem 2.6. *Let $A \subset F$. Then there is a collection of points P and lines L with $|P| = |A + A||A.A|$ and $|L| = |A|^2$ which has atleast $|A|^3$ incidences.*

Proof. Take $P = (A + A) \times (A.A)$, and let L be the lines of the form $l(a, b) := \{y = b(x - a)\}$, where $a, b \in A$.

Then note that $(a + c, bc) \in P$ in incident on $l(a, b)$ if $a, b, c \in A$. Hence any triplet from A constitutes an incidence. Therefore there are atleast $|A|^3$ incidences. □

From the above proof we see that in the above setting the number of incidences are atleast $|A|^3$. Hence if we can get a bound on the number of incidences in a general setting, we will be able to bound the number of incidences in the above setting and get a correspondingly get a sum-product estimate.

In the paper of Bourgain, Katz and tao [3], the similar bound for Szemeredi-Trotter problem in finite fields is proved, using the same proof structure, but there they use the sum-product estimate they derived, and which is stated above, to come at contradiction.

3 Counting Incidences over Reals

In this section, we will survey the bound on the number of incidences between a set of points and lines in the real space. The bound we present here is tight, unlike the finite field case, and cannot be improved, except in terms of the constansts involved.

The problem of counting incidences was first posed for the reals, and solved by Szemeredi and Trotter using the technique of cell decomposition [7]. However, a much simpler, which we present here, was developed later by Szekely [8]. The proof which we present can also be handle intersections between more complex objects. However, we do not cover these extensions and leave it upto the reader to look it up.

Theorem 3.1 (ST Theorem over reals)**.** *Let L be the set of M lines in $\mathbb{F}_p^2$ and let P be the set of N points in $\mathbb{R}_p^2$. Then* $|I(P, L)| = \mathcal{O}((NM)^{\frac{2}{3}} + N + M)$

The proof involves an elegant reduction of the problem to a graph problem and so before moving to the proof, we look into the notion of *drawing* and *crossing number* of a graph.

3.1 Crossing Number Inequality

Firstly let us recall Euler's formula for a planar graph,

$$|V| - |E| + |F| = 2$$

where F is the set of faces in the graph, including the unbounded one. As a corollary of Euler's formula, it can be proven that $|E| \leq 3|V| - 6$, for $|V| \geq 3$.

Consider a graph $G = (V, E)$ on the set of vertices V and edges $E \subset V \times V$. A *drawing* of a graph is a planar embedding of the graph in $\mathbb{R}^2$, with vertices represented as points and curves joining two vertices it there is an edge between them in the graph.

The crossing number of a particular drawing is the number of intersections in the drawing. The crossing number of the graph, denoted as $cr(G)$, is the minimum crossing number over all possible drawings. It is easy to see that a graph is planar, iff its crossing number is zero.

We next move to deriving the $crossing - number$ inequality, which gives a strong lower bound on $cr(G)$, given the number of edges.

Theorem 3.2 (Crossing Number inequality)**.** *Let G be a graph. If $|E| \geq 4|V|$, then*

$$cr(G) \geq \frac{|E|^3}{64|V|^2}$$

Before proving the crossing number inequality, we state and prove a much simpler bound on $cr(G)$, which we will then extend to get the above theorem.

Claim 3.1. *For any graph G, $cr(G) \geq |E| - 3|V|$*

Proof of claim 3.1. Observe that removing an edge would reduce the number of intersections and hence $cr(G)$ by atmost one. If we remove $cr(G)$ appropriate edges from the graph, we reduce the crossing number to zero, ie, the graph becomes planar. The new graph has $|V|$ vertices and $|E| - cr(G)$ edges.

Using the corollary of Euler's formula, for this new graph we have

$$|E| - cr(G) \leq 3|V|$$
$$\implies cr(G) \geq |E| - 3|V|$$

□

Proof of Crossing-Number inequality. A single crossing in the drawing of the graph G can be considered to involve 4 distince vertices of G, just like an edge is considered to involve 2 distince vertices of G. The main idea of the proof is that if we look at the random vertices induced subgraph of G, then this subgraph should also satisfy an inequality similar to the above claim.

From the above claim we have that,

$$cr(G) \geq |E| - 3|V|$$

Let $G' = (V', E')$ be the induced subgraph, formed using vertices from $V' \subset V$, where vertices in V' are chosen independently from V with probability $p \in [0, 1]$.

In that case, Claim 3.1 must also hold for G',

$$cr(G') \geq |E'| - 3|V'|$$

Taking expectations both sides, we get

$$\mathbb{E}[cr(G')] \geq \mathbb{E}[|E'|] - 3\mathbb{E}[|V'|]$$

Since the probability of choosing a vertex is p, we have that $\mathbb{E}[|V'|] = p|V|$. Again since an edge can represented by two distinct vertices of V, we have that $\mathbb{E}[|E'|] = p^2|E|$. Similarly, since a crossing can represented by four distinct vertices of V, we have that $\mathbb{E}[cr(G')] = p^4 cr(G)$.

Therefore, we get

$$p^4 cr(G) \geq p^2|E| - 3p|V|$$

If we now take $p = \frac{4|V|}{|E|}$ and solve the above equation along with the original claim for graph G, we get that

$$cr(G) \geq \frac{|E|^3}{64|V|^2}$$

□

3.2 Proof of Szemeredi-Trotter Theorem in Reals

Proof. We now prove the ST theorem for set P of N points and set L of M lines. It involves an elegant reduction of the problem to a graph problem. First we have all those lines that have atmost two incidence on them. This would have contributed atmost $2M$ to the total number of incidences and we will take them into consideration later.

We define $P(l)$ as before for each line $l \in L$,

$$P(l) = \{p \in P | p \in l\}$$

We can see that

$$|I(P, L)| = \sum_{l \in L} P(l)$$

Note that if a line contains k points, then it will have $k - 1$ line segments or atleast $k/2$ line segments, since in our case $k > 2$. Hence,

$$\frac{|I(P, L)|}{2} \leq \text{Number of line segments}$$

Consider our setting to be the drawing of a graph $G = (V, E)$ whose vertices V are the N points and there is an edge in the graph between two vertices if the corresponding points lie on the same line. Then each line segment represents an edge. Hence if we have a bound on number of edges, we get a bound on the number of incidences.

Note that since two lines intersect in atmost one point, the crossing number of this graph is $\leq M^2$. Applying the crossing-number inequality, we get that either $|E| \leq 4|V|$ or

$$M^2 \geq \frac{|E|^3}{64|V|^2}$$

$$\implies |I(P,L)| \leq c(NM)^{2/3}$$

Hence considering the above inequalities and assumptions,

$$|I(P,L)| = \mathcal{O}((NM)^{\frac{2}{3}} + N + M)$$

□

References

[1] Z. Dvir, *Incidence Theorems and Their Applications* (2013), http://arxiv.org/pdf/1208.5073v2.pdf

[2] S. Lovett, *Additive Combinatorics and its Applications in Theoretical Computer Science* (2013), http://cseweb.ucsd.edu/~slovett/files/addcomb-survey.pdf

[3] J. Bourgain, N. Katz, T. Tao, *A Sum-Product Estimate in Finite Fields, and Applications*, Geom. Func. Anal. 14 (2004). http://arxiv.org/pdf/math/0301343v3.pdf

[4] A. Balog and E. Szemeredi., *A statistical theorem of set addition*, Combinatorica (1994) 14(3):263-268.

[5] W. T. Gowers, *A new proof of Szemeredis theorem for arithmetic progressions of length four*, Geom. Funct. Anal. (1998), 17(2):230261.

[6] G. Elekes, *On the number of sums and products*, Acta Arith.(1997), 365367.

[7] E. Szemeredi and W.T. Trotter, *Extremal problems in discrete geometry*, Combinatorica (1983), **3**, 381392

[8] Szekely, A. Lszl, *Crossing numbers and hard Erds problems in discrete geometry*, Combinatorics, Probability and Computing (1997), **6**, 353-358.

[9] P. Erdos, E. Szemeredi, *On sums and products of integers*, Studies in Pure Mathematics (1983), 213-218

[10] J. Bourgain, *Multilinear exponential sums in prime elds under optimal entropy condition on the sources.*, Geometric And Functional Analysis (2009), 1477-1502