A COURSE IN ARITHMETIC COMBINATORICS

MICHAEL BJÖRKLUND

CONTENTS

1. IMPACT FUNCTIONS AND PLÜNNECKE'S THEOREM

Let G be a finite group and denote by m_G the normalized counting (Haar) measure on G, i.e.

$$m_G(B) = \frac{|B|}{|G|}, \quad \text{for all } B \subset G.$$

Given non-empty subsets $A, B \subset G$, we define the *product set* AB of A and B by

$$AB = \{ab : a \in A, b \in B\}.$$

We say that a set $A \subset G$ is a *basis* of order k if

$$A^k = A \cdot A \cdots A = G.$$

Note that a proper subgroup of G can never be a basis of any order.

Given a basis A of order k in G, we wish to understand in this lecture the rough behavior of the associated *impact function* ρ_A which is defined by

$$\rho_A(t) = \min\Big\{m_G(AB) : m_G(B) \geq t\Big\} \quad \text{for } 0 \leq t \leq 1.$$

1.1. **The Erdös-Raikov Inequality.** Suppose that $A \subset G$ contains at least two elements. We may assume that one of these elements is the identity and we note that

$$m_G(AB) \geq m_G(B \cup aB) = m_G(B) + m_G(aB \setminus B) \quad \text{for all } a \in A.$$

Define the *ejectivity function* ζ_A by

$$\zeta_A(t) = \inf\Big\{\varepsilon_A(B) : B \subset G \text{ such that } m_G(B) \geq t\Big\},$$

where

$$\varepsilon_A(B) = \sup_{a \in A} m_G(aB \setminus B),$$

so that

$$m_G(AB) \geq m_G(B) + \zeta_A(m_G(B)).$$

In particular, we have

$$\rho_A(t) \geq t + \zeta_A(t), \quad \text{for all } 0 \leq t \leq 1.$$

The following basic result (see the papers [1] and [5])) is sometimes referred to as the *Erdös-Raikov Inequality*.

Theorem 1.1. *Let G be a finite group and suppose $A \subset G$ is a basis of order k in G. Then*

$$\zeta_A(t) \geq \frac{1}{k} \cdot t \cdot (1-t) \quad \textit{for all } 0 \leq t \leq 1.$$

To prove this theorem, we shall need two lemmata.

Lemma 1.1. *For any $A \subset G$ and for every positive integer n, we have*

$$\zeta_{A^n}(t) \leq n \cdot \zeta_A(t)$$

for all $0 \leq t \leq 1$.

Proof. First note that if X, Y and Z are subsets of G, then

$$m_G(X \setminus Y) \leq m_G(X \setminus Z) + m_G(Z \setminus Y).$$

In particular, if we define the function

$$\xi(x) = m_G(xB \setminus B), \quad x \in G,$$

then

$$\xi(xy) \leq \xi(x) + \xi(y) \quad \text{for all } x, y \in G.$$

For any $x_1, \ldots, x_n$, we have

$$m_G(x_1 \cdots x_n B \setminus B) = \xi(x_1 \ldots x_n) \leq \xi(x_1) + \ldots + \xi(x_n) = m_G(x_1 B \setminus B) + \ldots m_G(x_n B \setminus B)$$

which readily implies the lemma. □

Lemma 1.2. *For every finite group G, we have*

$$\zeta_G(t) \geq t \cdot (1-t),$$

for all $0 \leq t \leq 1$.

Proof. One readily verifies that

$$\int_G m_G(B \cap xB)\, dm_G(x) = m_G(B)^2$$

for every $B \subset G$ and thus there exists at least one $x \in G$ such that

$$m_G(B \cap xB) \leq m_G(B)^2,$$

and thus

$$m_G(xB \setminus B) = m_G(B) - m_G(B \cap xB) \geq m_G(B) \cdot (1 - m_G(B)),$$

which finishes the proof. □

To prove Theorem 1.1: Let $A \subset G$ be a basis of order k. Then, by the lemmata above, we have

$$\zeta_A(t) \geq \frac{1}{k} \cdot \zeta_G(t) \geq \frac{1}{k} \cdot t \cdot (1-t)$$

for all $0 \leq t \leq 1$.

1.2. **Plünnecke's Inequality.** In the case when G is a finite *abelian* group, Plünnecke [4] was able to provide a better lower bound on the impact function for a basis of order k. In this subsection, we shall outline the recent argument by Petridis [3] to obtain this celebrated bound.

Theorem 1.2. *Let G be a finite* abelian *group and suppose A and B are non-empty subsets of G. Let $K \geq 1$ be a constant such that*

$$m_G(AB) \leq K \cdot m_G(B).$$

Then there exists a non-empty subset $B' \subset B$ such that

$$m_G(A^k B') \leq K^k \cdot m_G(B'), \quad \textit{for all } k.$$

In particular, if $A \subset G$ is a basis of order k, then

$$m_G(AB) \geq m_G(B)^{1-\frac{1}{k}} \quad \textit{for all } B \subset G,$$

or equivalently, $\rho_A(t) \geq t^{1-\frac{1}{k}}$ for all $0 \leq t \leq 1$.

We shall need the following lemma.

Lemma 1.3 (Petridis, [3]). *Let G be a finite* abelian *group and suppose A and B are non-empty subsets of G. Let $B' \subset B$ be a non-empty subset such that*

$$\frac{m_G(AB')}{m_G(B')} = \min\left\{\frac{m_G(AB'')}{m_G(B'')} : \emptyset \neq B'' \subset B\right\}.$$

Then, for every $F \subset G$, we have

$$m_G(FAB') \leq m_G(FB') \cdot \frac{m_G(AB')}{m_G(B')}. \tag{1.1}$$

Proof. Note that inequality (1.1) trivially holds whenever the set F consists of a single point. Our argument now goes as follows. Fix a finite set $F \subset G$ for which (1.1) holds and pick $g \in G \setminus F$. We shall prove that (1.1) then holds for the set $F' = F \cup \{g\}$.

Since G is abelian, we have the inclusion

$$A(B' \cap g^{-1}FB') \subseteq AB' \cap g^{-1}FAB',$$

and thus,

$$\begin{aligned} F'AB' &= FAB' \cup \left(gAB' \setminus FAB'\right) \\ &= FAB' \cup g\left(AB' \setminus (AB' \cap g^{-1}FAB')\right) \\ &\subseteq FAB' \cup g\left(AB' \setminus A(B' \cap g^{-1}FB')\right). \end{aligned}$$

Since $B' \cap g^{-1}FB' \subset B' \subset B$, we have

$$m_G(A(B' \cap g^{-1}FB')) \geq m_G\left(B' \cap g^{-1}FB'\right) \cdot \frac{m_G(AB')}{m_G(B')},$$

and thus

$$\begin{aligned} m_G\left(F'AB'\right) &\leq m_G(FAB') + \mu(AB') - m_G(A(B' \cap g^{-1}FB')) \\ &\leq m_G(FAB') + m_G(AB') - m_G(B' \cap g^{-1}FB') \cdot \frac{m_G(AB')}{m_G(B')} \\ &\leq m_G(FAB') + \left(m_G(B') - m_G(B' \cap g^{-1}FB')\right) \cdot \frac{m_G(AB')}{m_G(B')}. \end{aligned}$$

Since (1.1) is assumed to hold for the set F, we conclude that

$$m_G\big(F'AB'\big) \le \Big(m_G(FB') + m_G(B') - m_G(B' \cap g^{-1}FB')\Big) \cdot \frac{m_G(AB')}{m_G(B')}.$$

Note that

$$m_G(FB') + m_G(B') - m_G(B' \cap g^{-1}FB') = m_G(F'B),$$

which finishes the proof. □

Proof of Theorem 1.2. Let G be a finite abelian group and suppose A and B are non-empty subsets of G. Fix a non-empty subset $B' \subset B$ such that

$$K_o = \frac{m_G(AB')}{m_G(B')} = \min\left\{\frac{m_G(AB'')}{m_G(B'')} : \emptyset \neq B'' \subset B\right\} \le K.$$

We wish to prove that

$$m_G(A^kB) \le K_o^k \cdot m_G(B), \quad \text{for all } k.$$

Clearly this inequality holds for $k = 1$. Assume that

$$m_G(A^{k-1}B) \le K_o^{k-1} \cdot m_G(B), \quad \text{for some } k \ge 2.$$

Then, by Lemma 1.3 applied to the set $F = A^{k-1}$, we have

$$m_G(A^kB') \le K_o \cdot m_G(A^{k-1}B') \le K_o^k \cdot m_G(B'),$$

which finishes the proof of Theorem 1.2. □

In particular, if we apply Theorem 1.2 to the sets $A = B$ for some non-empty subset $B \subset G$, then we can find a non-empty subset $B' \subset B$ such that

$$m_G(B^k) \le m_G(B^kB') \le K^k \cdot m_G(B') \le K^k \cdot m_G(B),$$

whenever $m_G(B^2) \le K \cdot m_G(B)$. We have thus proved:

Corollary 1.1. *Let G be a finite abelian group and suppose*

$$m_G(B^2) \le K \cdot m_G(B)$$

for some constant K. Then $m_G(B^k) \le K^k \cdot m_G(B)$ for all k.

1.3. Ruzsa's Triangle Inequality.

Proposition 1.1. *Let G be a finite group and suppose that A and B are non-empty subsets of G. Let $K \ge 1$ be a constant such that $|AB| \le K \cdot |B|$. Then,*

$$|A^kA^{-l}| \le K^{k+l} \cdot |B|, \quad \textit{for all } k,l \ge 0.$$

Lemma 1.4.

1.4. **Failure of Plünnecke's inequality for non-abelian groups.** We shall now see that if we drop the assumption that G is an abelian group, then counterexamples to the conclusion of Corollary 1.1 are easy to come by.

We say that a subgroup $H < G$ is *locally malnormal* if

$$xHx^{-1} \cap H = \{e\} \quad \text{for some } x \in G \setminus H.$$

Note that abelian groups do not admit non-trivial locally malnormal subgroups.

Proposition 1.2. *Let G be a finite group which contains a proper locally malnormal subgroup $H < G$ with at least 33 elements. Then, for every $x \in G \setminus H$ such that $xHx^{-1} \cap H = \{e\}$, we have*

$$m_G(B_x^2) \le 3 \cdot m_G(B) \quad \textit{and} \quad m_G(B_x^3) > 27 \cdot m_G(B_x),$$

where $B_x = \{x\} \cup H$.

Proof. We first note that

$$B_x^2 = H \cup Hx \cup xH \cup \{x^2\} \quad \text{and} \quad B_x^3 \supset HxH,$$

for every $x \in G$, so in particular

$$m_G(B_x^2) \leq 3 \cdot m_G(B_x) \quad \text{and} \quad m_G(B_x^3) \geq m_G(HxH).$$

Since H is a locally malnormal subgroup, there exists $x \in G$ such that $xHx^{-1} \cap H = \{e\}$ and thus the identity $|HxH| = |H|^2$ holds. Indeed, one readily checks that the map $q : H \times H \to HxH$ given by

$$q(s,t) = sxt \quad (s,t) \in H \times H,$$

is bijective. In particular, if $m_G(B_x^3) \leq 27 \cdot m_G(B_x)$, then

$$27 \cdot (|H| + 1) \geq |H|^2,$$

which does not have a solution if $|H| \geq 33$. □

Typical examples of locally malnormal subgroups stem from semi-direct products. Let N and L be finite groups and suppose there exists a homomorphism $\alpha : L \to \mathrm{Aut}(N)$. The *semi-direct product* of N and L with respect to α shall be denoted by $G = N \rtimes_\alpha L$, and is given by the direct product of the sets N and L equipped with the multiplication

$$(x,s) \cdot (y,t) = (x\alpha(s)y, st), \quad \text{for all } (x,s),(y,t) \in G.$$

One readily checks that the subgroup $N \rtimes_\alpha \{e\}$ is normal in G and

$$\big(\{e\} \rtimes_\alpha L\big) \cap (y,e) \cdot \big(\{e\} \rtimes_\alpha L\big) \neq \{(e,e)\}$$

for some $y \in N \setminus \{e\}$ if and only if $\alpha(s)y = y$ for some $s \in L \setminus \{e\}$. In particular, if $\alpha(s)y \neq y$ for some y and for all non-trivial s (in which case we shall refer to α as *locally free*), then $\{e\} \rtimes_\alpha L$ is locally malnormal in G.

We end this lecture by the following observation.

Proposition 1.3. *Every finite group L admits an embedding into a finite group G such that its image is locally malnormal in G.*

To prove the proposition, it suffices to produce by the arguments above, for every finite group L, a finite group N and a locally free homomorphism $\alpha : L \to \mathrm{Aut}(N)$. For this purpose, let N denote the abelian group of all subsets of L equipped with the multiplication

$$A \cdot B = \big(A \setminus B\big) \cup \big(B \setminus A\big), \quad \text{for all } A, B \subset N.$$

Clearly, every element in N has order two and the empty set is the identity element in N. We can now choose

$$\alpha(s)B = sB, \quad \text{for all } s \in L \text{ and } B \subset L.$$

One checks that $\alpha(s)(A \cdot B) = \alpha(s)A \cdot \alpha(s)B$ for all $s \in L$ and $A, B \subset L$. In other words, each $\alpha(s)$ is an automorphism of N, and $\alpha(s)\{e\} = \{s\} \neq \{e\}$ for every non-trivial $s \in L$, which shows that α is locally free, and thus $\{e\} \rtimes_\alpha L$ is subnormal in G.

2. Small product sets

The aim of this lecture is to understand the structure of pairs of subsets (A,B) of a finite group G such that

$$m_G(AB) \leq K \cdot m_G(B) \tag{2.1}$$

for *small* values of K. The following important result by M. Kneser allows us to gain some understanding in the case when $K < \frac{3}{2}$ and G is abelian.

If G is a finite group and $C \subset G$ is a non-empty subset, then the (left) *stabilizer* $\mathrm{Stab}_G(C)$ of the set C is defined by

$$\mathrm{Stab}_G(C) = \{g \in G : gC = C\}.$$

Theorem 2.1 (Kneser, Satz 1 in [2]). *Let G be a finite* abelian *group and suppose that $A,B \subset G$ are non-empty subsets. Then*

$$m_G(AB) \geq \min\big(1, m_G(AH) + m_G(BH) - m_G(H)\big),$$

where H denotes the stabilizer group of AB. In particular, if the stabilizer of AB is trivial, then

$$|AB| \geq \min\big(|G|, |A| + |B| - 1\big), \quad \textit{for all } A,B \subset G.$$

Remark 2.1. Since m_G is a probability measure, it is clearly necessary to stress that the right hand side in the first inequality above does not exceed one. However, we also note that if

$$m_G(A) + m_G(B) > 1,$$

then $AB = G$. Indeed, suppose this does not hold. Then there exists $x \notin AB$ and thus $A^{-1}x$ and B are disjoint sets, which forces

$$1 \geq m_G(A^{-1}x \cup B) = m_G(A) + m_G(B) > 1,$$

which is a contradiction. Hence we may always assume that $m_G(A) + m_G(B) - m_G(H) < 1$.

The proof of Theorem 2.1 is rather technical, so we first collect a few immediate consequences of the theorem in order motivate it.

Since the finite abelian groups $\mathbb{Z}/p\mathbb{Z}$ lack non-trivial proper subgroups when p is a prime number, we conclude:

Corollary 2.1 (Cauchy-Davenport's Theorem). *Let p be a prime. Then,*

$$|AB| \geq \min\big(p, |A| + |B| - 1\big), \quad \textit{for all } A,B \subset \mathbb{Z}/p\mathbb{Z}.$$

We shall now show how Kneser's Theorem can be used to deduce structural information about pairs of subsets (A,B) as in (2.1) with $K < \frac{3}{2}$.

Corollary 2.2. *Let G be a finite abelian group and suppose that A and B are subsets of G which satisfy $B \subset A$ and*

$$m_G(AB) < \frac{3}{2} \cdot m_G(B).$$

Then there exists a subgroup $H < G$ with $|H| < \frac{3}{2} \cdot |B|$ such that B is contained in a coset of H.

Proof. Let H denote the stabilizer of AB and note that $AB = (AH)(BH)$. Hence, by Theorem 2.1 and the inclusion $B \subset A$, we have

$$\frac{3}{2} \cdot |BH| > \frac{3}{2} \cdot |B| > |AB| \geq 2 \cdot |BH| - |H|,$$

which implies that $|BH| < 2 \cdot |H|$ and thus B must be contained in a coset of H. In particular, this forces the bound

$$\frac{3}{2} \cdot |B| > 2|H| - |H|,$$

and we conclude that $|H| < \frac{3}{2} \cdot |B|$. □

2.1. **A local version of Theorem 2.1.** The proof of Kneser's Theorem is quite involved and will use an elaborate form of induction. We formulate in this subsection a "local version" of this theorem, which will immediately imply Theorem 2.1, and whose proof will occupy most of the remaining part of this section.

Proposition 2.1 (Local version I of Kneser's Theorem)**.** *Let G be a finite abelian group and suppose A and B are non-empty subsets of G. For every non-empty subset $X \subset AB$, there exists a subset $C \subset AB$, which contains X such that*

$$m_G(C) \geq \min\Big(1, m_G(A) + m_G(B) - m_G(\mathrm{Stab}_G(C))\Big).$$

In particular, by taking $X = AB = (AH)(BH)$ where H denotes the stabilizer of AB, we can conclude that

$$m_G(AB) \geq \min\Big(1, m_G(AH) + m_G(BH) - m_G(H)\Big),$$

for all $A, B \subset G$.

2.2. **Proof of Proposition 2.1.** In this subsection we break down the proof of the local version of Kneser's Theorem into two parts.

We begin by stating the following special case (corresponding to the case when $|X| = 1$ in Proposition 2.1), whose proof will be given in the next subsection.

Proposition 2.2 (Local version II of Kneser's Theroem)**.** *Let G be a finite abelian group and suppose A and B are non-empty subsets of G. For every $x \in AB$, there exists $C \subset AB$, which contains x such that*

$$m_G(C) \geq \min\Big(1, m_G(A) + m_G(B) - m_G(\mathrm{Stab}_G(C))\Big).$$

The following technical lemma will also be useful.

Lemma 2.1. *Let G be a finite (not necessarily abelian) group and suppose that H_1 and H_2 are two normal subgroups of G. If*

$$C_1 = F_1 H_1 \quad \textit{and} \quad C_2 = F_2 H_2,$$

for some subsets $F_1 \subset G/H_1$ and $F_2 \subset G/H_2$, and if neither C_1 nor C_2 is contained in the other, then either

$$|C_1 \setminus C_2| \geq |H_2 \setminus H_1| \quad \textit{or} \quad |C_2 \setminus C_1| \geq |H_1 \setminus H_2|.$$

We can now give the proof of the local version of Kneser's Theorem.

Proof of Proposition 2.1. We shall use induction over the size of $X \subset AB$. For $|X| = 1$, then Proposition 2.1 follows from Proposition 2.2.

Suppose that we have established Proposition 2.1 for all subsets $X \subset AB$ with $|X| \leq k - 1$ for some $k \geq 2$. We wish to prove that it then holds for all sets with k elements.

Pick $X \subset AB$ with $|X| = k$ and write $X = X_1 \cup X_2$ with $|X_1|, |X_2| < k$. Then Proposition 2.2 produces

$$X_1 \subset C_1 \subset AB \quad \text{and} \quad X_2 \subset C_2 \subset AB$$

with

$$|C_1| \geq |A| + |B| - |H_1| \quad \text{and} \quad |C_2| \geq |A| + |B| - |H_2|,$$

where H_1 and H_2 denotes the stabilizers of C_1 and C_2 respectively (we assume henceforth that the right hand sides are all strictly less than $|G|$). Furthermore, we can write

$$C_1 = F_1 H_1 \quad \text{and} \quad C_2 = F_2 H_2$$

for some subsets $F_1 \subset G/H_1$ and $F_2 \subset G/H_2$. Now, if $C_1 \subset C_2$, then we can choose $C = C_2$ and

$$|C| \geq |A| + |B| - |H_2|,$$

and similarly if $C_2 \subset C_1$. Hence the important case to consider is when neither C_1 nor C_2 is contained in the other. By Lemma 2.1, we then have either

$$|C_1 \setminus C_2| \geq |H_2 \setminus H_1| \quad \text{or} \quad |C_2 \setminus C_1| \geq |H_1 \setminus H_2|.$$

If the first inequality holds, then we take $C = C_1 \cup C_2$ and note that

$$H = \mathrm{Stab}_G(C) \supset H_1 \cap H_2$$

which implies that

$$\begin{aligned} |C| &= |C_1 \cup C_2| \\ &= |C_2| + |C_1 \setminus C_2| \\ &\geq |A| + |B| - |H_2| + |H_2 \setminus H_1| \\ &= |A| + |B| - |H_1 \cap H_2| \geq |A| + |B| - |H|. \end{aligned}$$

The argument for the second inequality is completely identical, which finishes the proof. □

2.3. **Dyson transforms and the proof of Proposition 2.2.** Given a pair (A, B) of non-empty subsets of a finite abelian group G with $e \in A \cap B$ and an element $x \in A$, we define the *Dyson transform* (A', B') by

$$A' = A \cup Bx \quad \text{and} \quad B' = x^{-1}A \cap B.$$

One readily checks that $A \subset A'$ and $\emptyset \neq B' \subset B$ and

$$A'B' \subset AB \quad \text{and} \quad |A'| + |B'| = |A| + |B|.$$

Set $A_o = A$ and B_o and $x_1 = x$ for some fixed element $x \in A$ and define recursively the Dyson transforms

$$A_k = A_{k-1} \cup x_k B_{k-1} \quad \text{and} \quad B_k = x_k^{-1} A_{k-1} \cap B_{k-1}$$

for some choices of $x_k \in A_{k-1}$. We note that

$$A_{k-1} \subset A_k \quad \text{and} \quad B_k \subset B_{k-1} \quad \text{and} \quad A_k B_k \subset AB$$

and

$$|A_k| + |B_k| = |A_{k-1}| + |A_{k-1}| = |A| + |B|$$

for all k. Since G is finite, there exists an integer k such that

$$B_k = x^{-1} A_k \cap B_k \quad \text{for all } x \in A_k,$$

or equivalently, $A_k y = A_k$ for all $y \in B_k$. In other words, B_k is contained in the stabilizer of the set A_k.

Hence, if we set $C = A_k$, then $x \in C$, and

$$|C| = |A_k| = |A| + |B| - |B_k| \geq |A| + |B| - |\mathrm{Stab}_G(C)|,$$

which finishes the proof of Theorem 2.2. We note that $A_k \subset A_k B_k \subset AB$ and thus the right hand side is always strictly less than or equal to $|G|$.

3. Freiman's Theorem for finite groups (Lecture by Hegarty)

Theorem 3.1 (A special case of Freiman's Theorem)**.** *Let G be a finite* abelian *group and suppose that A and B are non-empty subsets. Let $K \geq 1$ be a constant such that $m_G(AB) \leq K \cdot m_G(B)$, and set*

$$\beta = \frac{m_G(B)}{m_G(A)}.$$

Then there exists a subgroup $H < G$ which contains A and such that

$$|H| \leq K^2 \cdot \beta \cdot |G|^{K^4 \cdot \beta} \cdot |A|.$$

See the proof of Theorem 2.1 in
`http://www.math.cmu.edu/~af1p/Teaching/AdditiveCombinatorics/Additive-Combinatorics.pdf`

4. Roth's Theorem (Lecture by Roginskaya)

See Subsection 6.5.2 in:

`http://staff.polito.it/danilo.bazzanella/PhD_files/Not%20always%20buried%20deep%20(Pollack).pdf`

5. Schur's Theorem

The aim of this lecture is to prove an old theorem of I. Schur from 1916 which asserts that Fermat's famous equations

$$s^n + t^n = u^n, \quad n \geq 1,$$

are always solvable in the finite fields $\mathbb{F}_p$, provided that the characteristic p is large enough in terms of n. More precisely:

Theorem 5.1 (Schur)**.** *For every $n \geq 1$, there exists an integer S_n such that for every prime number $p > S_n$, the equation*

$$s^n + t^n = u^n$$

admits a solution (s,t,u) in $\mathbb{F}_p$ such that $stu \neq 0$.

Given $n \geq 1$, we define the subgroup

$$G_n = \{s^n : s \in \mathbb{F}_p^*\},$$

where $\mathbb{F}_p^*$ denotes the multiplicative group of $\mathbb{F}_p$ which we shall sometimes identify with the subset $\{1,\ldots,p-1\}$ in $\mathbb{F}_p$. We note that

$$\mathbb{F}_p^* = \{1,\ldots,p-1\} = a_1 G_n \sqcup \ldots \sqcup a_k G_n,$$

for some elements $a_1,\ldots,a_k \in \mathbb{F}_p^*$. Schur's Theorem is now an immediate consequence of the following proposition.

Proposition 5.1. *For every $k \geq 1$, there exists a number T_k such that whenever $N \geq T_k$ and*

$$\{1,\ldots,N\} = A_1 \sqcup \ldots \sqcup A_k$$

is any k-partition, then there exists an index $i = 1,\ldots,k$ such that the equation $x+y=z$ is solvable with $x,y,z \in A_i$.

Indeed, choose a prime number p larger than $T_n > T_k$. By the proposition, applied to the partition $A_i = a_i G_n$, with $i = 1, \ldots, k$, we can find an index i and $x, y, z \in A_i$ such that $x + y = z$, or equivalently,

$$a_i s^n + a_i t^n = a_i u^n$$

for some $s, t, u \in \mathbb{F}_p^*$ and clearly, $stu \neq 0$ in $\mathbb{F}_p$.

To prove Proposition 5.1, we shall need the following version of Ramsey's Theorem.

Theorem 5.2. *For every $k, m \geq 1$, there exists a number $n = n(k, m)$ such that for any k-coloring of the complete graph with n vertices, there is a monochromatic complete subgraph on m vertices.*

We note that if

$$\{1, \ldots, N\} = A_1 \sqcup \ldots \sqcup A_k$$

is a partition, then $|j - i| \in \{1, \ldots, N - 1\}$ for every $1 \leq i, j \leq N$, and

$$c(i, j) = l \quad \text{if } |j - i| \in A_l$$

is a coloring of the complete graph on N vertices.

Suppose that $N > n(k, 3)$. Then, by Ramsey's Theorem above, there exists a color, say l, and three vertices $i, j, m \in \{1, \ldots, N$ in color l with $i < j < m$. Hence, if we let

$$x = m - j \quad \text{and} \quad y = j - i \quad \text{and} \quad x = m - i,$$

then x, y and z belong to the partition element A_l and

$$x + y = z,$$

which proves Proposition 5.1.

5.1. **Proof of Theorem 5.2.** We shall first establish the following infinite version of Ramsey's Theorem:

Proposition 5.2. *For every $k \geq 1$ and for every k-edge-coloring of an infinite complete graph, there exists an* infinite *monochromatic complete subgraph.*

It is not hard to see that it suffices to prove this proposition for two colors, say green and red.

Proof for $k = 2$. We argue greedily. Let V be the vertex set of an infinite complete graph, whose edges are colored in green and red, and pick a vertex $v_1 \in V = V_1$. Either this vertex has infinitely many outgoing green edges or it has infinitely many red outgoing edges. Suppose that we are in the first case and let V_2 denote the set of these vertices which are endpoints of gree edges from v_1. There are now two cases:

First case: There exists a vertex $v_2 \in V_2$ with infinitely many green edges to vertices in V_2. Let V_3 denote this set. Continue inductively: If there exists a vertex $v_3 \in V_3$ with infinitely many green edges to vertices in V_3, then we let V_4 denote this set, and so forth. If this process can go on indefinitely, then the complete subgraph with vertices $v_1, v_2, v_3, \ldots$ is green.

Second case: Assume that the process described under the first case terminates after a finite number of steps, i.e. there exists n such that every vertex in V_n only has finitely many green edges emanating. Then we can change colors and run the first case. However, the "red" process will not terminate since every vertex in V_n only has finitely many green outgoing edges. □

5.2. **Pushing to infinite sets.** We now deduce the Theorem 5.2 from Proposition 5.2. For this we shall need the following compactness observation.

Proposition 5.3. *Let $\mathscr{F}$ be a family of finite subsets of $\mathbb{N}$ such that for any k-coloring of $\mathbb{N}$, there exists a monochromatic subset in $\mathscr{F}$. Then there exists $n = n(k)$ such that for every k-coloring of $\{1,\dots,n\}$, there is in $\mathscr{F}$ a monochromatic subset.*

Proof. We argue by contradiction. For every n, let c_n be a k-coloring of $\{1,\dots,n\}$ such that no element in $\mathscr{F}$ is monochromatic with respect to c_n. Let i_1 be a color such that the set

$$I_1 = \{n \geq 1 : c_n(1) = i_1\}$$

is infinite. Inductively, we can choose colors $i_2, i_3, \dots$ such that the sets

$$I_m = \{n \geq m : c_n(1) = i_1, c_n(2) = i_2, \dots, c_n(m) = i_m\}$$

are all infinite. If we set $c(m) = i_m$ for all $m \geq 1$, then c is a k-coloring of $\mathbb{N}$, so by assumption, there exists a color i and a set $F \in \mathscr{F}$ such that

$$F \subset c^{-1}(i).$$

Since F is finite, it must be contained in $\{1,\dots,m\}$ for some m. Fix $n \in I_m$. Then c coincides with c_n on $\{1,\dots,m\}$, but by assumption, c_n does not admit a monochromatic subset in $\mathscr{F}$, which leads to a contradiction. □

6. van der Waerden's Theorem

Read Subsection 6.2.2. in:

http://staff.polito.it/danilo.bazzanella/PhD_files/Not%20always%20buried%20deep%20(Pollack).pdf

7. Quasi-randomness and Gowers' Theorem

The aim of this lecture is to prove the following special case of a theorem by T. Gowers. Recall that if F is a field, then $\mathrm{PSL}_2(F)$ denotes the quotient of $\mathrm{SL}_2(F)$ with its center, i.e. all matrices of the form $\pm I$.

Theorem 7.1 (Gowers' Quasi-Randomness Theorem)**.** *For every prime number $p > 3$ and for every subset $A \subset \mathrm{PSL}_2(\mathbb{F}_p)$ with $|A| > |\mathrm{PSL}_2(\mathbb{F}_p)|^{\frac{8}{9}}$, we have $A^3 = G$.*

Let G be a finite group. A homomorphism $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ for some n is often called a (linear) *representation* of G. If $V \subset \mathbb{C}^n$ is a linear subspace such that $\rho(s)V = V$ for all $s \in G$, then we say that V is a *sub-representation* of ρ, and if ρ does not admit any non-trivial sub-representations (i.e. different from the trivial subspace and the whole $\mathbb{C}^n$), then we say that ρ is *irreducible*.

If ρ is a representation of G and $\langle \cdot, \cdot \rangle$ denotes the hermitian inner product on $\mathbb{C}^n$, then

$$\langle u, v \rangle_\rho := \frac{1}{|G|} \sum_{s \in G} \langle \rho(s)u, \rho(s)v \rangle, \quad u, v \in \mathbb{C}^n$$

is again a hermitian inner product on $\mathbb{C}^n$ with the property that

$$\langle \rho(t)u, \rho(t)v \rangle_\rho = \langle u, v \rangle_\rho$$

for all $t \in G$ and $u, v \in \mathbb{C}^n$.

We note that if V is a sub-representation of ρ, then its orthogonal subspace $V^{\perp}$ with respect to $\langle\cdot,\cdot\rangle_{\rho}$, i.e.

$$V^{\perp} = \{u \in \mathbb{C}^n : \langle u, v\rangle_{\rho} = 0, \quad \text{for all } v \in V\},$$

is also a sub-representation of ρ, and $\mathbb{C}^n = V \oplus V^{\perp}$. In particular, given any linear representation $\rho : G \to \mathrm{GL}_n(\mathbb{C})$, we can write

$$\mathbb{C}^n = \bigoplus_{i=1}^{k} V_i,$$

where this decomposition is orthogonal with respect to $\langle\cdot,\cdot\rangle_{\rho}$, and each V_i is an *irreducible* representation of G. Here is a simple, yet important lemma.

Lemma 7.1. *If G is abelian, then any irreducible representation ρ is one-dimensional.*

Proof. Pick any non-trivial element $s \in G$, and let v be an eigenvector for $\rho(s)$ with eigenvalue λ. Hence, the linear subspace

$$V_{\lambda} = \{w \in \mathbb{C}^n : \rho(s)w = \lambda w\}$$

is non-trivial, and since G is abelian, V_{λ} is a sub-representation. Indeed, for any $t \in G$, we have

$$\rho(s)\rho(t)w = \rho(t)\rho(s)w = \lambda\rho(t)w,$$

which shows that $\rho(t)V_{\lambda} = V_{\lambda}$ for every t. This means that $\rho(s)$ equals $\lambda \cdot I$. Since s is arbitrary, we conclude that there must exist a homomorphism $\lambda : G \to \mathbb{C}^*$ such that $\rho(s) = \lambda(s) \cdot I$ for every s in G. We have assumed that ρ is irreducible, and thus we must conclude that $n = 1$, since otherwise would any proper sub-space be invariant under this representation. □

We note that we can identify one-dimensional representations (which are of course automatically irreducible) of a finite group G with homomorphisms $\chi : G \to \mathbb{C}^*$. Indeed, we see that

$$\rho_{\chi}(g)z = \chi(g)z \quad \text{for all } z \in \mathbb{C}$$

is a one-dimensional representation of G. In particular, if we take $\chi = 1$, then we recover the identity representation on $\mathbb{C}$.

Gowers Theorem is a straightforward consequence of the following two lemmata. We denote by $d(G)$ to be the *minimal* dimension of a non-trivial (linear) representation of a G.

Lemma 7.2 (Frobenius)**.** *For every prime $p > 3$, we have $d(\mathrm{PSL}_2(\mathbb{F}_p)) \geq \frac{p-1}{2}$.*

Lemma 7.3 (Gowers expansion)**.** *For every finite group G and for all subsets $A, B, C \subset G$ with $|A| \cdot |B \cdot |C| > |G|^3/d(G)$, we have $ABC = G$.*

Combining these two lemmata in the special case when $A = B = C$ yields Gowers Theorem.

7.1. **Proof of Lemma 7.2.** A fundamental role will be played by the abelian subgroup

$$U = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in \mathbb{F}_p \right\} < \mathrm{PSL}_2(\mathbb{F}_p),$$

which is clearly isomorphic to the additive group $\mathbb{F}_p$. A straightforward calculations shows that

$$N(U) = \{g \in \mathrm{PSL}_2(\mathbb{F}_p) : gUg^{-1} = U\} = \left\{ \begin{pmatrix} \alpha & x \\ 0 & \alpha^{-1} \end{pmatrix} : \alpha \in \mathbb{F}_p^*, x \in \mathbb{F}_p \right\} < \mathrm{PSL}_2(\mathbb{F}_p),$$

where α and $-\alpha$ have been identified. In particular, we have

$$|N(U)/U| \geq \frac{p-1}{2}.$$

Suppose that ρ is a representation of $\mathrm{PSL}_2(\mathbb{F}_p)$ of dimension n, different from the identity representation. We wish to show that $n \geq \frac{p-1}{2}$. We argue as follows. Since U is abelian, Lemma 7.1 tells us that we may write

$$\mathbb{C}^n = \bigoplus_{i=1}^{m} V_{\chi_i},$$

where χ_i are homomorphisms from U into $\mathbb{C}^*$ and

$$V_{\chi_i} = \{v \in \mathbb{C}^n : \rho(u)v = \chi_i(u)v \quad \text{for all } u \in U\}.$$

We stress that V_{χ_i} will NOT be a sub-representation for ρ, but only for the restriction of ρ to U. However, if $g \in N(U)$ and $v \in V_{\chi_i}$, then

$$\rho(u)\rho(g)v = \rho(g)\rho(g^{-1}ug)v = \chi_i(g^{-1}ug)\rho(g)v,$$

which shows that $\rho(g)V_{\chi_i} = V_{\rho(g)\chi_i}$, where

$$(\rho(g)\chi_i)(u) = \chi_i(g^{-1}ug), \quad \text{for } u \in U.$$

In other words, the restriction of ρ to the normalizer $N(U)$ of U permutes the decomposition above. In particular,

$$\mathbb{C}^n \supset \bigoplus_{T \in \rho(N(U))/\rho(U)} V_{T\chi_i}$$

for every i, (one has to check that the stabilizer of every χ_i equals U), which readily implies that

$$n \geq \left|\rho(N(U)/U)\right|,$$

since each $V_{T\chi_i}$ is at least one-dimensional.

What saves us now is:

Lemma 7.4. *For every prime $p > 3$, the group* $\mathrm{PSL}_2(\mathbb{F}_p)$ *is simple, i.e. it does not admit any non-trivial* normal *subgroups.*

Hence, by this lemma, the kernel of ρ (which is a normal subgroup of G) must be either trivial or the whole of G (in which case ρ is the identity representation). Since we have assumed that ρ is not the identity representation we conclude that ρ is injective, and thus

$$n \geq \left|\rho(N(U)/U)\right| = \left|N(U)/U\right| \geq \frac{p-1}{2}.$$

7.2. **Proof of Lemma 7.3.** Given a function $f : G \to \mathbb{C}$ and a linear representation ρ of G of dimension n, we define the operator

$$\rho(f)v = \sum_{s \in G} f(s)\rho(s)v, \quad v \in \mathbb{C}^n.$$

In particular, if ρ denotes the identity representation, then

$$\rho(f)v = \big(\sum_s f(s)\big) \cdot v$$

The convolution of two functions $f_1, f_2 : G \to \mathbb{C}^n$ is defined by

$$(f_1 * f_2)(g) = \sum_{st=g} f_1(s) f_2(t).$$

Note that

$$\rho(f_1 * f_2)v = \sum_g \sum_{st=g} f_1(s) f_2(t)\rho(s)\rho(t)v = \rho(f_1)\rho(f_2)v.$$

Denote by $\hat{G}$ the set of irreducible representations of G, and write d_ρ for the dimension of ρ. We shall need the following lemma, which we leave as an exercise.

Lemma 7.5. *For every $f : G \to \mathbb{C}$, we have*

$$f(g) = \frac{1}{|G|} \sum_{\rho \in \hat{G}} d_\rho \, \mathrm{tr}(\rho(g)^* \rho(f)),$$

where tr *denotes the standard trace on $n \times n$-matrices, and the transpose of $\rho(g)$ is taken with respect to the inner product $\langle \cdot, \cdot \rangle_\rho$. In particular, we have*

$$\sum_{g \in G} |f(g)|^2 = \frac{1}{|G|} \sum_{\rho \in \hat{G}} d_\rho \cdot \|\rho(f)\|^2,$$

where $\|T\|^2 = \mathrm{tr}(T^* T)$.

In particular, we have

$$|A| = \sum_{g \in G} |\chi_A(g)|^2 = \frac{1}{|G|} \sum_{\rho \in \hat{G}} d_\rho \cdot \|\rho(\chi_A)\|^2,$$

for every subset $A \subset G$, which means that

$$\|\rho(\chi_A)\| \leq \sqrt{\frac{|A| \cdot |G|}{d_\rho}} \leq \sqrt{\frac{|A| \cdot |G|}{d(G)}}$$

for every non-trivial ρ. Again, if ρ is the identity (trivial) representation, then $\rho(\chi_A) = |A|$.

We wish to prove that if $A, B, C \subset G$ with $|A| \cdot |B| \cdot |C| \geq |G|^3 / d(G)$, then $ABC = G$, or equivalently

$$\chi_A * \chi_B * \chi_C(g) > 0 \quad \text{for all } g \in G.$$

By Lemma 7.5 and the formulas above, we have, by the Cauchy-Schwartz inequality,

$$\chi_A * \chi_B * \chi_C(g) \geq \frac{|A| \cdot |B \cdot |C|}{|G|} - \frac{1}{|G|} \sum_{\rho \neq id} d_\rho \|\chi(\chi_A)\| \cdot \|\rho(\chi_B)\| \cdot \|\rho(\chi_C)\|.$$

Plugging in the bounds above, and using Cauchy-Schwartz Inequality again,

$$\begin{aligned}
\chi_A * \chi_B * \chi_C(g) &\geq \frac{|A| \cdot |B \cdot |C|}{|G|} - \sqrt{\frac{|A| \cdot |G|}{d(G)}} \cdot \frac{1}{|G|} \sum_{\rho \neq id} d_\rho \cdot \|\rho(\chi_B)\| \cdot \|\rho(\chi_C)\| \\
&\geq \frac{1}{|G|} \cdot \Big(|A||B||C| - \sqrt{\frac{|A| \cdot |G|}{d(G)}} \Big(\sum_{\pi \neq id} d_\rho \cdot \|\rho(\chi_B)\|^2 \Big)^{\frac{1}{2}} \cdot \Big(\sum_{\pi \neq id} d_\rho \cdot \|\rho(\chi_C)\|^2 \Big)^{\frac{1}{2}} \Big) \\
&\geq \frac{1}{|G|} \cdot \Big(|A||B||C| - \sqrt{\frac{|A| \cdot |G|}{d(G)}} \cdot |G| \cdot \sqrt{|B| \cdot |C|} \Big),
\end{aligned}$$

where in the last inequality we used Lemma 7.5 to deal with the remaining $\|\rho(\chi_B)\|$ and $\|\rho(\chi_C)\|$. For the last expression to be positive, it suffices that

$$|A||B||C| > \frac{|G|^{3/2}}{\sqrt{d(G)}} \cdot \sqrt{|A||B||C|},$$

or equivalently $|A| \cdot |B| \cdot |C| > |G|^3 / d(G)$, which finishes the proof of Lemma 7.3.

7.3. **Proof of Lemma 7.4.** A nice exposition of the proof (using a criterion by Iwasawa) can be found under:

```
http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/PSLnsimple.pdf
```

8. A Sum-Product Theorem (Lecture notes by Hegarty)

Throughout this lecture, unless otherwise stated, all sets are subsets of $\mathbb{R}_+$.

Recall that if A is any set of positive real numbers, then the sumset $A+A$, the product set $A\cdot A$ and the quotient set $\frac{A}{A}$ are defined as

$$A+A=\{a_1+a_2 : a_1,a_2\in A\}, \tag{8.1}$$

$$A\cdot A=\{a_1a_2 : a_1,a_2\in A\}, \tag{8.2}$$

$$\frac{A}{A}=\left\{\frac{a_1}{a_2} : a_1,a_2\in A\right\}. \tag{8.3}$$

If A is a finite set, $|A|=n$ say, then

$$2n-1\le |A+A|\le \frac{n(n+1)}{2}, \tag{8.4}$$

$$2n-1\le |A\cdot A|\le \frac{n(n+1)}{2}, \tag{8.5}$$

$$2n-1\le \left|\frac{A}{A}\right|\le n(n-1)+1. \tag{8.6}$$

The right-hand inequalities are proven by considering the total number of possible sums, products resp. quotients and noting that addition and multiplication are commutative whereas division is not. The left-hand inequality for the sumset is verified by observing that, if $A=\{a_1<a_2<\cdots<a_n\}$, then there is a strictly increasing sequence of $2n-1$ sums formed by

$$a_1+a_1<a_1+a_2<\cdots<a_1+a_n<a_2+a_n<\cdots<a_n+a_n. \tag{8.7}$$

Similar arguments give the left-hand inequalities for the product and quotient sets.

We are interested primarily in the sum and product sets. The lower bound in (0.1) is attained by an arithmetic progression and in (0.2) by a geometric progression. These are two quite different types of sets, however. The core of the *sum-product phenomenon* is that the sumset and product set cannot simoultaneously be small. The usual reference for a precise formulation of this idea is the following famous conjecture:

Conjecture 1. (Erdős-Szemerédi conjecture, 1982) *For every $\varepsilon>0$ there exists an absolute positive constant C_ε such that, if A is a finite set of real numbers then*

$$\max\{|A+A|,|A\cdot A|\}\ge C_\varepsilon|A|^{2-\varepsilon}. \tag{8.8}$$

Below we will prove the strongest result to date in this direction (Theorem 0.11). Firstly, however, we show that one cannot take $\varepsilon=0$ in the E-S conjecture, i.e.: there is no absolute positive constant C_0 such that $\max\{|A+A|,|A\cdot A|\}\ge C_0|A|^2$.

Theorem 8.1. (Erdős Multiplication Table Theorem) *Let $A=\{1,2,\dots,n\}$. Then $|A\cdot A|=o(n^2)$.*

The proof of this combines some estimates about prime numbers with a probabilistic method. These "standard" results can be summarised in the following two lemmas:

Lemma 8.1. *For any $x\ge 2$,*

$$\sum_{p\le x}\frac{1}{p}=\log\log x+b+O\left(\frac{1}{\log x}\right), \tag{8.9}$$

where b is some constant.

Proof. See Theorem 6.4 in the lecture notes for my course in number theory:

http://www.math.chalmers.se/~hegarty/mma300_ht14.html □

Lemma 8.2. *If X is a real-valued random variable with finite mean μ and finite variance σ^2, then for any $\lambda > 0$,*

$$\mathbb{P}(|X-\mu| \geq \lambda) \leq \frac{\sigma^2}{\lambda^2}. \tag{8.10}$$

Proof. This is known as *Chebyshev's inequality* and a proof can be found in any introductory textbook on probability theory. For a good introduction specifically to the probabilistic method in combinatorics, see the book "The Probabilistic Method", by Noga Alon and Joel Spencer. □

Before proceeding, we note two immediate corollaries of Lemma 0.3:

Corollary 8.1. *For any $x \geq 2$,*

$$\sum_{p^a \leq x, a \in \mathbb{N}} \frac{1}{p^a} = \log\log x + b' + O\left(\frac{1}{\log x}\right), \tag{8.11}$$

where b' is some constant.

Proof. One has

$$\sum_{p^a \leq x, a \geq 2} \frac{1}{p^a} = \sum_{p^a, a \geq 2} \frac{1}{p^a} - \sum_{p^a > x, a \geq 2} \frac{1}{p^a} \tag{8.12}$$

and it is easy to see that the first sum on the right is convergent, while the second is $O(1/x)$. □

Corollary 8.2.

$$\sum_{p^a, q^b \leq x} \frac{1}{p^a q^b} \leq \left(\log\log x + b' + O\left(\frac{1}{\log x}\right)\right)^2. \tag{8.13}$$

Proof. The sum on the left of (0.13) is bounded above by the square of the sum on the left of (0.9). Note that the two are not identical, since cross-terms would be counted twice in the latter. □

For $n \in \mathbb{N}$ define $\Omega(n)$ to be the number of prime power divisors of n. So, for example, $\Omega(36) = 4$ since the prime powers dividing 36 are $2, 3, 2^2$ and 3^2. Note that $\Omega(1) = 0$. The Fundamental Theorem of Arithmetic implies that

$$\Omega(ab) = \Omega(a) + \Omega(b), \quad \text{for all } a, b \in \mathbb{N}. \tag{8.14}$$

The main step in the proof of Theorem 0.2 is the following:

Proposition 8.1. *For every $\varepsilon > 0$, there exists $N_\varepsilon \in \mathbb{N}$ such that, if $N > N_\varepsilon$ and the number n is chosen uniformaly at random from $\{1, 2, \ldots, N\}$, then*

$$\mathbb{P}((1-\varepsilon)\log\log N < \Omega(n) < (1+\varepsilon)\log\log N) > 1 - \varepsilon. \tag{8.15}$$

Proof. Fix $N \in \mathbb{N}$, let X be a number from $\{1, 2, \ldots, N\}$ chosen uniformly at random and $Y := \Omega(X)$. Thus Y is a non-negative integer valued random variable. The idea of the probabilstic method is to compute the first and second moments of Y and then use Lemma 0.4. Regarding the first moment one has

$$\mathbb{E}(Y) = \frac{1}{N}\sum_{n=1}^{N} \Omega(n) = \frac{1}{N}\sum_{n=1}^{N}\sum_{p^a|n} 1 =$$

$$= \frac{1}{N}\sum_{p^a \leq N} \lfloor \frac{N}{p^a} \rfloor = \sum_{p^a \leq N} \frac{1}{p^a} + O(1) = \log\log x + O(1), \tag{8.16}$$

by Lemma 0.3. For the second moment,

$$\mathbb{E}(Y^2) = \frac{1}{N}\sum_{n=1}^{N}\left(\sum_{p^a|n} 1\right)^2 = \frac{1}{N}\sum_{n=1}^{N}\sum_{p^a|n,\, q^b|n} 1 =$$
$$= \sum_{p^a \leq N,\, q^b \leq N} \#\{n \leq N : p^a|n,\, q^b|n\}.$$

We consider three different contributions to the double-sum:

CASE 1: $p = q$, $a = b$. Then the sum is just the first moment $\mathbb{E}(Y)$.

CASE 2: $p = q$, $a < b$. This contribution will be

$$\frac{1}{N}\sum_{q^b \leq N,\, b \geq 2} (b-1)\cdot \lfloor \frac{N}{q^b} \rfloor, \tag{8.17}$$

where the factor $b-1$ comes from the fact that there are so many choices for q^a, given q^b and $a < b$. It is easy to see that this sum is $O(1)$. We will get an equal contribution from terms with $p = q$ and $a > b$.

CASE 3: $p \neq q$. Then the double sum becomes

$$\frac{1}{N}\sum_{p^a \leq N,\, q^b \leq N,\, p \neq q} \lfloor \frac{N}{p^a q^b} \rfloor \leq \sum_{p^a \leq N,\, q^b \leq N} \frac{1}{p^a q^b} \leq \left(\log\log N + b' + O\left(\frac{1}{\log N}\right)\right)^2, \tag{8.18}$$

by Corollary 0.5. To summarise, we have shown that

$$\mathbb{E}(Y^2) \leq \mathbb{E}(Y) + O(1) + \left(\log\log N + b' + O\left(\frac{1}{\log N}\right)\right)^2. \tag{8.19}$$

Combining this with (0.16), it follows that

$$\mathrm{Var}(Y) = \mathbb{E}(Y^2) - (\mathbb{E}(Y))^2 = \log\log N + O(1). \tag{8.20}$$

Let $\mu := \mathbb{E}(Y)$ and $\sigma^2 := \mathrm{Var}(Y)$. Thus $\mu = \log\log N + O(1)$ and $\sigma^2 = \log\log N + O(1)$ also. For any fixed $\varepsilon > 0$, by Lemma 0.4 with $\lambda = \varepsilon\mu$ one has

$$\mathbb{P}(|Y - \mu| > \varepsilon\mu) \leq \frac{\sigma^2}{\varepsilon^2\mu^2} \lesssim \frac{1}{\varepsilon^2 \log\log N} < \varepsilon, \tag{8.21}$$

provided N is sufficiently large. This completes the proof of the proposition. □

Theorem 0.2 follows easily from the proposition. Basically, the point is that for n large, "most" products of two numbers from $\{1, 2\ldots, n\}$ will, by (0.14) and the Proposition, result in numbers with approximately $2\log\log n$ prime power divisors, whereas "most" numbers in $\{1, 2, \ldots, n^2\}$ have approximately $\log\log n^2 \sim \log\log n$ prime power divisors. Hence, "most" numbers in the latter set cannot be such products. I leave it to the reader to fill in the details of a rigorous proof.

We now turn to positive results on the E-S conjecture. First, let me reformulate it in a more convenient form:

Conjecture 2. *For every $\delta \in (0,1)$ there exists an absolute positive constant C_δ such that, if A is a finite set of real numbers then*

$$\max\{|A + A|, |A \cdot A|\} \geq C_\delta |A|^{1+\delta}. \tag{8.22}$$

There are basically six quantum leaps in progress which people refer to:

ERDŐS-SZEMERÉDI (1982): In their original paper, they proved that the conjecture holds for *some* $\delta > 0$, but they did not give any explicit constant.

NATHANSON (1997): Proved that the conjecture holds for $\delta = 1/31$, by carefully analysing the original argument of Erdős and Szemerédi.

FORD (1998): Proved the conjecture for $\delta = 1/15$, by further modifying Nathanson's presentation.

ELEKES (1997): Proved the conjecture for $\delta = 1/4$. The argument here is quite different and employs as a black box a fundamental result from incidence geometry called the *Szemerédi-Trotter theorem*, see below.

SOLYMOSI (2005): Proved the conjecture for $\delta = 3/11$. This proof also uses the Szemerédi-Trotter theorem, but in a slightly more sophisticated way.

SOLYMOSI (2009): Proved the conjecture for $\delta = 1/3 - \varepsilon$ and any $\varepsilon > 0$. This result surprised people when it first appeared because, like previous works, it uses a geometrical argument (points and lines in $\mathbb{R}^2$), but NOT the Sz-Tr theorem. Thus it showed that such point-line arguments could be pushed further than people previously thought.

We will sketch the proof of Elekes, using Sz-Tr as a black box (his paper is 2 pages long !) and then give a full proof of Solymosi's 2009 result. The latter can also be found in [S].

The following is the form of the Sz-Tr theorem which was directly applied by Elekes:

Theorem 8.2. (Szemerédi-Trotter, 1983) *There is an absolute constant $C > 0$ such that, for all pairs n, k of positive integers, given n points in the plane, the number of lines each containing at least k of them is at most $C(n^2/k^3 + n/k)$.*

Remark 8.1. The term n^2/k^3 can be thought of as the main term, since it will dominate for all $k \leq \sqrt{n}$. The non-trivial thing here is that the power of k in the denominator is greater than 2. A bound of $O(n^2/k^2)$ could be obtained by a simple double-count, upon noting that any two points determine a line uniquely.

Proof. of Elekes result. Let $A = \{a_1 < a_2 < \dots a_n\}$. For each $1 \leq j, k \leq n$ let $f_{j,k} : \mathbb{R} \to \mathbb{R}$ be the function

$$f_{j,k}(x) = a_j(x - a_k). \tag{8.23}$$

Note that, for any $1 \leq i \leq n$, $f_{j,k}(a_k + a_i) = a_j a_i$. Thue the graph of each function

$$y = a_j(x - a_k) \tag{8.24}$$

contains at least n points of the set $\mathscr{P} = (A + A) \times (A \cdot A)$. Let $N := |\mathscr{P}|$. Each such graph is of course a line. We have n^2 lines and thus, by Szemerédi-Trotter, there is a constant C such that $n^2 \leq C(N^2/n^3 + N/n)$. Since $N \geq (2n-1)^2$, by (0.1) and (0.2), we see that N^2/n^3 is the main term and easily deduce that $N \geq C' n^{5/2}$ for some $C' > 0$. By definition of the set $\mathscr{P}$, it follows that

$$\max\{|A + A|, |A \cdot A|\} \geq C''|A|^{5/4}, \quad \text{for some absolute } C'' > 0\text{, v.s.v.} \tag{8.25}$$

□

We now turn to Solymosi's 2009 result. For a real number x, denote $\lceil\lceil x \rceil\rceil := \lfloor x \rfloor + 1$. What he actually proved is

Theorem 8.3. (Solymosi 2009) *If A is a finite set of positive real numbers then*

$$|A \cdot A||A+A|^2 \geq \frac{|A|^4}{4\lceil\lceil \log|A| \rceil\rceil}. \tag{8.26}$$

Note the immediate corollary that

$$\max\{|A+A|, |A \cdot A|\} \geq \frac{|A|^{4/3}}{4^{1/3}\lceil\lceil \log|A| \rceil\rceil^{1/3}}. \tag{8.27}$$

The proof of Theorem 0.11 invokes the (well-known) concept of *multiplicative energy*[1]. Let A be a set of positive reals. The multiplicative energy of A, denoted $E_\times(A)$, is defined as

$$E_\times(A) = \#\{(a_1, a_2, a_3, a_4) \in A^4 : a_1/a_2 = a_3/a_4\}. \tag{8.28}$$

Solymosi's Lemma. *If A is a set of positive reals, then*

$$\frac{E_\times(A)}{\lceil\lceil \log|A| \rceil\rceil} \leq 4|A+A|^2. \tag{8.29}$$

The lemma quickly implies the theorem. Let $\pi_1, \dots, \pi_t$ be the distinct elements of the product set $A \cdot A$, and let $n_1, \dots, n_t$ respectively denote the number of representations of each element as a product, i.e.: $n_i = \#\{(a_1, a_2) \in A^2 : a_1 a_2 = \pi_i\}$. Thus, by definition, $|A|^2 = \sum_{i=1}^t n_i$ and $E_\times(A) = \sum_{i=1}^t n_i^2$. By the Cauchy-Schwarz inequality,

$$E_\times(A) = \sum_{i=1}^t n_i^2 \geq \frac{1}{t}\left(\sum_{i=1}^t n_i\right)^2 = \frac{|A|^4}{|A \cdot A|}. \tag{8.30}$$

Plugging this into (0.29) immediately yields (0.26).

So it remains to prove Solymosi's lemma.

Write

$$E_\times(A) = \sum_{i=0}^{\lfloor \log|A| \rfloor} \sum_{2^i \leq |xA \cap A| < 2^{i+1}, x \in A/A} |xA \cap A|^2. \tag{8.31}$$

Note that this is correct, since if $x = a_1/a_2$ say and $a_3 \in xA \cap A$, then it means there exists $a_4 \in A$ such that $\frac{a_1}{a_2}a_4 = a_3$, hence that $a_1/a_2 = a_3/a_4$. Thus, the double sum on the right counts every 4-tuple of elements of A contributing to $E_\times(A)$ exactly once.

By the pigeonhole principle, there must be some $I \in \{0, \dots, \lfloor \log|A| \rfloor\}$ such that

$$\frac{E_\times(A)}{\lceil\lceil \log|A| \rceil\rceil} \leq \sum_{2^I \leq |xA \cap A| < 2^{I+1}, x \in A/A} |xA \cap A|^2. \tag{8.32}$$

Let $D := \{s \in A/A : 2^I \leq |sA \cap A| < 2^{I+1}\}$ and let $s_1 < s_2 < \cdots < s_m$ denote the elements of D in increasing order. First note that (0.32) immediately implies that

$$\frac{E_\times(A)}{\lceil\lceil \log|A| \rceil\rceil} < m \cdot 2^{2I+2}. \tag{8.33}$$

On the other hand, for each $j = 1, \dots, m$, let l_j be the line $y = s_j x$. Consider the Cartesian product $A \times A$ as a set of points in $\mathbb{R}^2$. By definition, the number of points of $A \times A$ contained in each l_j is somewhere in the interval $[2^I, 2^{I+1})$. Let l_{m+1} be the vertical line through a_1, the smallest element of A. Thus l_{m+1} contains exactly $|A|$ points from $A \times A$, namely the points (a_1, a_j),

[1] There is an analogous concept of *additive energy,* defined exactly as you would expect given (0.28).

$j = 1, \dots, |A|$. The point now is that

(i) for each $1 \le j < k \le m+1$,

$$|(l_j \cap (A \times A)) \oplus (l_k \cap (A \times A))| = |l_j \cap (A \times A)| \cdot |l_k \cap (A \times A)|, \tag{8.34}$$

were $\oplus$ denotes vector addition in $\mathbb{R}^2$.

(ii) the sumsets along consecutive line pairs are disjoint.

Both (i) and (ii) are seen most easily by drawing a picture - see [S]. The point is that all points in the sumset $(l_j \cap (A \times A)) \oplus (l_{j+1} \cap (A \times A))$ lie in the segment of the plane bounded by l_j and l_{j+1}, which implies (ii). For (i) we just need the fact that any two vectors along l_j and l_{j+1} are linearly independent.

Thirdly, by definition of vector addition one has

(iii) for all j, k,

$$(l_j \cap (A \times A)) \oplus (l_k \cap (A \times A)) \subseteq (A+A) \times (A+A). \tag{8.35}$$

Putting (i), (ii) and (iii) together yields

$$m \cdot 2^{2I} \le \left| \bigcup_{j=1}^{m} \big(l_j \cap (A \times A)\big) \oplus \big(l_{j+1} \cap (A \times A)\big) \right| \le |A+A|^2. \tag{8.36}$$

From this and (0.33) we deduce (0.29).

9. Home work assignments

Exercise 1. Let G be a finite group. Recall that a subset $A \subset G$ is a *basis of order* k if $A^k = G$. Since we always have the bound $|A^k| \le |A|^k$ for any subset $A \subset G$, we see that a basis of order k must necessarily satisfy $|A| \ge |G|^{\frac{1}{k}}$. The aim of the first exercise is to show that this is essentially sharp.

Fix $0 < p < 1$ and let (ε_x) be a family of independent $\{0,1\}$-variables indexed by $x \in G$ and which attain the value 1 with probability p. Define the random subset

$$A = \{x \in G : \varepsilon_x = 1\} \subset G.$$

Show that for every $\varepsilon > 0$, there exists a finite group G (e.g. $G = \mathbb{Z}/m\mathbb{Z}$ for some integer m) and a subset $A_o \subset G$ such that $A_o A_o^{-1} = G$ and

$$|A_o| \le |G|^{\frac{1}{2}+\varepsilon}.$$

Hint: Choose $p = |G|^{-\alpha}$ *and vary* $|G|$ *and* α.

Exercise 2. Apply a similar argument as in Exercise 1 to show that for any subset $B \subset G$, there exists $F \subset G$ such that $FB = G$ with

$$|F| \le C \cdot \frac{|G|}{|B|} \cdot \log|G|$$

for some constant C which is independent of G and B.

Now over to something completely different: Recall that Schur's Theorem asserts that the equations

$$x^n + y^n = z^n$$

are solvable in $\mathbb{F}_p$, provided that p is large enough with respect to n. Our proof was completely ineffective. The aim of the following exercise is to remedy this inefficiency by giving a more direct Fourier-analytic proof.

We begin by setting up the terminology. Given a prime number p, we define

$$e_p(x) = e^{2\pi i \frac{x}{p}}, \quad x \in \mathbb{F}_p$$

and

$$S(k) = \sum_{x \in \mathbb{F}_p} e_p(kx^n), \quad k \in \mathbb{F}_p.$$

Show that

$$N = \left|\{(x,y) \in \mathbb{F}_p : x^n = y^n\}\right| = \frac{1}{p} \sum_{k \in \mathbb{F}_p} |S(k)|^2$$

and $N \leq 1 + np$.

Define

$$M_p = \sum_{x,y,z \in \mathbb{F}_p} \frac{1}{p} \sum_{k \in \mathbb{F}_p} e_p(k(x^n + y^n - z^n)$$

Exercise 3. Prove that

$$|M_p| \geq \frac{1}{2}p^2 \quad \text{if } p \geq 16n^6 \text{ (or just something bounded below by } n)$$

and show that this bound implies that there exists $x, y, z \in \mathbb{F}_p$ with $x^n + y^n = z^n$ and $xyz \neq 0$.

Hint: Prove that

$$M_p = \frac{1}{p} \sum_{k \in \mathbb{F}_p} S(k)^2 \overline{S(k)},$$

and

$$|S(k)| \leq \sqrt{2p} \cdot n, \quad \text{for all } k \neq 0.$$

Exercise 4.

References

1. P. Erdös, *On the arithmetical density of the sum of two sequences, one of which forms a basis for the integers*, Acta Arithmetica, **1** (1936), 201–207.
2. M. Kneser, *Summenmengen in lokalkompakten abelschen Gruppen.* (German) Math. Z. **66** (1956), 88–110.
3. G. Petridis, *New proofs for Plünnecke-type Estimates for product sets in groups*. http://arxiv.org/abs/1101.3507
4. H. Plünnecke. *Eine zahlentheoretische anwendung der graphtheorie.* J. Reine Angew. Math., 243:171–183, 1970.
5. D. A. Raikov, *On the addition of point sets in the sense of Schnirelmann*, Mat. Sbornik, **5**(47) (1939), 425–440, (in Russian).

S. J. Solymosi, Bounding multiplicative energy by the sumset, *Advances in Mathematics* **222** (2009), No. 1, 402–408.

Department of Mathematics, Chalmers, Gothenburg, Sweden
E-mail address: micbjo@chalmers.se