Roth's Theorem for Finite Groups

Presented by Hein Thant AUNG

28 February, 2023

The classic Roth's theorem [4] states that any subset $A \subseteq \mathbb{N}$ of positive upper density contains an arithmetic progression of length 3. One way to improve the notion of 'positive upper density' is to introudce the number $r_3(n)$, the size of the largest subset of $\{1, 2, \ldots, n\}$ not containing a 3-term arithmetic progression. Under this notation, the classic Roth's theorem says that $r_3(n) = o(n)$. This bound has been improved over time with the current world record being

$$r_3(n) \leq \frac{n}{\exp(c(\log n)^{1/11})}$$

for some absolute constant $c > 0$, achieved by Bloom, Sisask, Kelly and Meka in 2023 February (preprint) [1]. Nevertheless, the goal of this presentation is to discuss some extensions of Roth's theorem for general groups.

The main highlight of this presentation is the following theorem, proven in [6] which we will present in section 2. Here, $\text{Syl}_2(K)$ denotes a (possibly trivial) Sylow 2-subgroup of K.

Theorem 1. (Roth's Theorem for Finite Groups) For every $\varepsilon > 0$, there is a positive integer M for every group G having a subgroup K with $[K : \text{Syl}_2(K)] \geq M$, any subset $S \subset G$ with $|S| \geq \varepsilon|G|$ contains three distinct elements b, db, d^2b where $d \in K$.

Another way to generalize an arithmetic progression into general groups is as a triplet $(x, y, z) \in G^3$ of group elements such that $xz = y^2$. One weakness of such generalization is that the property of being AP-free is no longer translation invariant: if $xz = y^2$, it is not necessarily true that $(ax)(az) = (ay)^2$ for any $a \in G$. The following theorems proven in [5], although we are not discussing today, are worth of mentioning when it comes to this direction.

Theorem 2. Let G be a finite group of order n. Let $A_1, \ldots, A_m$ with $m \geq 2$ be sets of elements of G and let g be an arbitrary element of G. If the equation

$$x_1 x_2 \ldots x_m = g \qquad \text{(eq. 1)}$$

has $o(n^{m-1})$ solutions with $x_i \in A_i$, then there are subsets $A_i' \subseteq A_i$ with $|A_i \setminus A_i'| = o(n)$ such that there is no solution of the equation (eq. 1) with $x_i \in A_i'$.

Corollary 3. Let G be a finite group of odd order n and $A \subseteq G$ be a subset. If the number of solutions to the equation $xz = y^2$ with $x, y, z \in A$ is $o(n^2)$, then the size of A is $o(n)$.

1 Necessary Tools

The central tool used to prove the theorems mentioned above is the triangle removal lemma (more generally, hypergraph removal lemma) from extremal graph theory.

Theorem 4. (Triangle Removal Lemma, version 1) For every $\varepsilon > 0$, there exists $\delta > 0$ such that every graph Γ containing at most $\delta|\Gamma|^3$ triangles can be made triangle-free by removing at most $\varepsilon|\Gamma|^2$ edges.

Vaguely saying, every graph with $o(|\Gamma|^3)$ triangles can be made triangle free by removing $o(|\Gamma|^2)$ edges. One possible approach to prove theorem 4 is via Szemeredi's Regularity Lemma (see for example [7]). But to my knowledge, this theorem is surprisingly difficult to prove. The version of triangle removal lemma we are going to be using today is the following.

Theorem 5. (Triangle Removal Lemma, version 2) For every $\varepsilon > 0$, there exists $\delta > 0$ such that every graph Γ containing at least $\varepsilon|\Gamma|^2$ edge-disjoint triangles will also contain at least $\delta|\Gamma|^3$ triangles.

First, let's see why these two versions are equivalent. Suppose theorem 4 is correct, and suppose we are given $\varepsilon > 0$. Choose the $\delta > 0$ guaranteed by theorem 4 with $\varepsilon/2$ in place of ε. Then, G must contain more than $\delta|\Gamma|^3$ triangles or otherwise, it can be made triangle free by removing $\varepsilon|\Gamma|^2/2$ edges. However, this is impossible as we need to remove at least one edge from $\varepsilon|\Gamma|^2$ edge-disjoint triangles to make Γ triangle-free. Now, suppose theorem 5 is correct, and suppose we are given $\varepsilon > 0$. Take $\delta > 0$ guaranteed by theorem 5 with $\varepsilon/3$ in place of ε. Consider the maximal collection Δ of edge-disjoint triangles in Γ. By theorem 5, we know that $|\Delta| \leq \varepsilon|\Gamma|^2/3$. By maximality, every triangle shares an edge with some triangle in Δ. Thus, removing all $3|\Delta| \leq \varepsilon|\Gamma|^2$ edges from all triangles in Δ will make Γ triangle-free.

Triangle removal lemma is notorious for having terrible bounds (i.e. bounds of δ in terms of ε) and thus putting a curse on every proof that makes use of the lemma. One known upper bound for $1/\delta$ is that it is bounded below by a tower of twos of height $O(\log(1/\varepsilon))$ and the current best known lower bound for $1/\delta$ is that it is bounded above by $\varepsilon^{-O(\log(1/\varepsilon))}$. Hence, there is a ginormous difference between lower and upper bounds.

Another tool that we will need are the two classic lemmas of Erdös and Strauss stating about the existence of large abelian subgroups in given finite groups. We shall state them here without proof.

Lemma 6. (Erdös and Strauss [2]) Let G be a finite group of order n. Then, G contains an abelian p-group P of order $\log n - o(\log n)$ as a subgroup.

The bound in lemma 6 is not tight. In fact, Pyber [3] has shown that there is a universal constant c such that every group of order n contains an abelian subgroup of order at least $2^{c\sqrt{\log n}}$. This bound is essentially tight.

2 Patterns in Large Subsets of $G \times G$

By a natural application of triangle removal lemma, we can prove the following lemma.

Lemma 7. For every $\varepsilon > 0$, there is a positive integer m such that whenever H is a subgroup of a finite group G with $|H| \geq m$, any set $S \subseteq G \times G$ with $|S| \geq \varepsilon |G|^2$ contains three elements (a, b), (ad, b) and (a, db) where $d \in H$.

Proof. For the given $\varepsilon > 0$, take the δ guranteed by theorem 5. Pick m so that the inequality $\delta X^3 > \varepsilon X^2$ holds for all $X \geq m$. Now, note that there exists $l, r \in G$ such that

$$|(lH \times Hr) \cap S| \geq \varepsilon |H|^2.$$

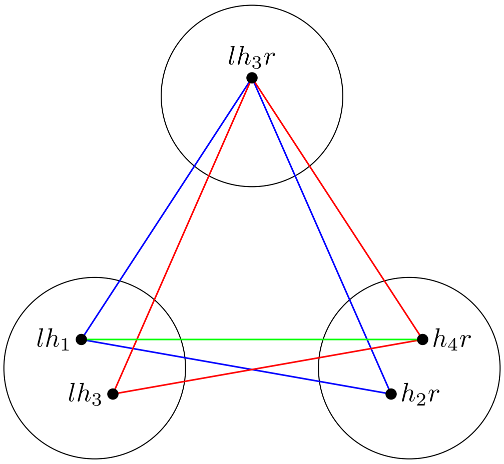
To see this, note that there are $(|G|/|H|)^2$ possible sets of the form $lH \times Hr$ and therefore, one of them contains at least

$$\frac{|S|}{|G|^2/|H|^2} = \frac{|S|}{|G|^2} \cdot |H|^2 \geq \varepsilon |H|^2$$

elements of S. Now, cerate a tripartite graph Γ with three vertex partitions: lH, Hr and lHr. We shall add edges to Γ as follows: go through all possible pairs $(g_1, g_2) \in (lH \times Hr) \cap S$ one by one. For each such pair, add the edges (g_1, g_2) from lH to Hr, $(g_1 g_2, g_2)$ from lHr to Hr and $(g_1 g_2, g_1)$ from lHr to lH. So there can be two types of triangles in Γ: those formed by the three edges that we add in some step (which we will call *original*) triangles and other triangles (g_1, g_2, g_3) with $g_1 g_2 \neq g_3$. Note that Γ contains at least $|S| \geq \varepsilon |G|^2$ original triangles which are all edge-disjoint. Therefore, by theorem 5, it contains $\delta |G|^3 > \varepsilon |G|^2$ triangles. In particular, it contains an non-original triangle. Thus, it contains 3 distinct triangles $(lh_1, h_2 r, lh_3 r)$, $(lh_1, h_4 r, lh_3 r)$ and $(lh_5, h_2 r, lh_3 r)$ with each $h_i \in H$ satisfying

$$h_1 h_2 \neq h_3, \quad h_3 = h_1 h_4 = h_5 h_2 \quad \text{and} \quad (lh_1, h_2 r), (lh_1, h_4 r), (lh_5, h_2 r) \in S$$

The conclusion follows by choosing $a = lh_1$, $b = h_2 r$ and $d = h_1^{-1} h_5 = h_4 h_2^{-1}$. □



We may now prove the next theorem, the proof of which can yield us theorem 1.

Theorem 8. For every $\varepsilon > 0$, there is a positive integer n such that for any finite group G with order at least n, any set $S \subseteq G \times G$ with $|S| \geq \varepsilon |G|^2$ contains three elements (a, b), (a, c) and (e, f) such that $ab = ec$ and $ac = ef$.

Proof. Let $\varepsilon > 0$ be given. We will make the choice of n later. By lemma 6, we know that G contains an abelian group H of size at least $\log(n)$. Let $l, r \in G$ be such that

$$|(lH \times Hr) \cap S| \geq \varepsilon |H|^2.$$

Write $L = lH$, $R = Hr$, $K = lHr$ and construct the tri-partite graph Γ on vertex sets L, R and K as in lemma 7. Then, by theorem 5, Γ contains at least $\delta'|H|^3$ non-original triangles where δ' is a constant only depending on ε and δ. Now, for each non-original triangle T, we can find three distinct triangles (a_T, b_T, c_T), (x_T, b_T, c_T) and (a_T, y_T, c_T) such that

$$a_T b_T \neq c_T, \quad c_T = x_T b_T = a_T y_T \quad \text{and} \quad (a_T, b_T), (x_T, b_T), (a_T, y_T) \in S.$$

Thus, there is a vertex $x \in L$ such that $x = x_T$ for at least $\delta'|H|^2$ non-original triangles T. We now construct a new tri-partite graph Γ' whose vertex set is A, B, C where A, B and C are the sets of elements of the form a_T, $a_T b_T$ and c_T respectively where T is a non-original triangle with $x = x_T$. We then add the edges $(a_T, a_T b_T)$, $(a_T b_T, c_T)$ and (a_T, c_T). Note that any two of $a_T, a_T b_T$ and c_T determine the other due to the relations:

$$c_T = x b_T = a_T y_T.$$

Therefore, Γ' contains at least $\delta'|H|^2$ triangles and again by theorem 5, if $|H|$ is large enough, there exist a triangle which is not of the form $(a_T, a_T b_T, c_T)$ for some non-original triangle T with $x = x_T$. Suppose that the edges of this triangle in Γ' are determined by distinct triangles T_1, T_2, T_3 in Γ with $x = x_{T_i}$ for $i = 1, 2, 3$ and

$$a_{T_1} = a_{T_3}, \quad c_{T_2} = c_{T_3}, \quad a_{T_1} b_{T_1} = a_{T_2} b_{T_2}.$$

This is all we need, so it's time to wrap up. We claim that choosing

$$(a, b) = (a_{T_1}, y_{T_1}), \quad (a, c) = (a_{T_3}, y_{T_3}) \quad \text{and} \quad (e, f) = (a_{T_2}, y_{T_2})$$

does the job. Indeed, they all belong to S and

$$ac = a_{T_1} y_{T_3} = a_{T_3} y_{T_3} = c_{T_3} = c_{T_2} = a_{T_2} y_{T_2} = ef.$$

To prove the remaining identity $ab = ec$, note that it is equivalent to

$$c_{T_1} = a_{T_2} a_{T_1}^{-1} c_{T_3}.$$

Since $c_{T_1} = x b_{T_1}$ and $c_{T_3} = x b_{T_3}$, it suffices to show that

$$x b_{T_1} = a_{T_2} a_{T_1}^{-1} x b_{T_3}.$$

Now, write $a_{T_1} = l\alpha_1$, $a_{T_2} = l\alpha_2$, $x = l\alpha_x$, $b_{T_1} = \beta_1 r$ and $b_{T_3} = \beta_3 r$ where $\alpha_1, \alpha_2, \alpha_x, \beta_1$ and β_3 are elements of H. Then, we need to show that

$$l\alpha_x \beta_1 r = l\alpha_2 \alpha_1^{-1} \alpha_x \beta_3 r.$$

But, this is true since H is abelian and $a_{T_1} b_{T_1} = a_{T_2} b_{T_2}$. □

Note that the terms b, c, f form an arithmetic progression with common difference $e^{-1}a \in H$. The only thing we need to worry now with regards to proving theorem 1 is when $e^{-1}a$ has degree 2.

This condition will be ruled out if we can choose H to be an arbitrarily large abelian subgroup of odd order. Here are the details:

Proof of Theorem 1. For an arbitrary $\varepsilon > 0$, and m be the positive integer guaranteed by lemma 7 with $S \times S$ replacing S. Let K be any subgroup of G with $|K : \mathrm{Syl}_2(K)| \geq M$. Then, by prime factorization of $|K|$ we can see that K contains a p-group P of order at least $(\log M)/2$ with $p \neq 2$ for sufficiently large M. But, by lemma 6, P has an abelian subgroup of size at least $(\log |P|)/2$ for some absolute constant $C > 0$. Therefore, K contains an abelian subgroup H with

$$|H| \geq (\log |P|)/2 \geq ((\log \log M) - \log 2)/2.$$

We can now follow the proof of lemma 8 to prove our theorem. □

The author of [6] conjectured that the following stronger version of theorem 8 holds:

Conjecture 9. For every $\varepsilon > 0$, there is a positive integer n such that if G is a finite group of order $|G| \geq n$, then any set $S \subseteq G \times G$ with $|S| \geq \varepsilon |G|^2$ contains four elements (a, b), (a, c), (e, c) and (e, f) such that $ab = ec$ and $ac = ef$.

3 Bonus: Proof of Roth's Theorem

To illustrate the power of triangle removal lemma, we will prove Roth's theorem i.e. $r_3(n) = o(n)$ using lemma 5.

Theorem 10. (Roth's Theorem) Any subset $A \subseteq \mathbb{N}_0$ of positive upper density contains an arithmetic progression of length 3.

Proof. (from [7]) Suppose that $A_n = A \cap \{0, 1, 2, \dots, n\}$ does not contain a 3-term AP for all positive integers n, and suppose to the contrary that there is some $\varepsilon > 0$ such that $|A_n| \geq \varepsilon n$ for sufficiently large n. We may embed A_n as a subset of $\mathbb{Z}/(2n+1)\mathbb{Z}$ by direct inclusion. Then, A_n still does not contain a 3-term AP as a subset of $\mathbb{Z}/(2n+1)\mathbb{Z}$. From now on, all the operations will be done inside $\mathbb{Z}/(2n+1)\mathbb{Z}$. Construct a tri-partite graph Γ with vertex set $X \sqcup Y \sqcup Z$ where $X = Y = Z = \mathbb{Z}/(2n+1)\mathbb{Z}$. We add edges in Γ as follows:

- $(x, y) \in X \times Y$ is an edge iff $y - x \in A_n$,
- $(y, z) \in Y \times Z$ is an edge iff $z - y \in A_n$,
- $(z, x) \in Z \times X$ is an edge iff $(z - x)/2 \in A_n$ where $1/2$ is the multiplicative inverse of 2 in $\mathbb{Z}/(2n+1)\mathbb{Z}$.

Now, since $y - x, (z - x)/2, z - y$ form an AP, every triangle in Γ corresponds to a trivial AP in A_n. More precisely, (x, y, z) is a triangle if and only if $y - x = z - y \in A_n$. So, all triangles in Γ are edge disjoint and there are exactly(!) $(2n+1)|A_n|$ of them. Hence, for sufficiently large n, by triangle removal lemma, Γ is going to contain $\delta(2n+1)^3$ triangles for some $\delta > 0$. But then, $|A_n| \geq (2n+1)^2$, contradiction. □

References

[1] Thomas F Bloom and Olof Sisask. "The Kelley–Meka bounds for sets free of three-term arithmetic progressions". In: *arXiv preprint arXiv:2302.07211* (2023).

[2] P Erdös and EG Straus. "How abelian is a finite group?" In: *Linear and Multilinear Algebra* 3.4 (1976), pp. 307–312.

[3] László Pyber. "How abelian is a finite group?" In: *The Mathematics of Paul Erdös I* (1997), pp. 372–384.

[4] Klaus F Roth. "On certain sets of integers". In: *J. London Math. Soc* 28.1 (1953), pp. 104–109.

[5] Oriol Serra, Lluis Vena, et al. "A combinatorial proof of the removal lemma for groups". In: *Journal of Combinatorial Theory, Series A* 116.4 (2009), pp. 971–978.

[6] Jozsef Solymosi. "Roth-type theorems in finite groups". In: *European Journal of Combinatorics* 34.8 (2013), pp. 1454–1458.

[7] Yufei Zhao. *Lecture Notes on Graph Theory and Additive Combinatorics for MIT 18.217 (Fall 2019).* 2019. URL: `https://ocw.mit.edu/courses/18-217-graph-theory-and-additive-combinatorics-fall-2019/pages/lecture-notes/`.