The Size of Progression-Free Sets in Non-Abelian Groups

Jay Reagan

Department of Mathematics
University of Pennsylvania

Master's Thesis Defense, 2017

An Introduction to the Problem

What is a progression-free set?

The simplest case:

- Let A be an additively written abelian group and let B be a subset of A. A triple of elements $a, b, c \in B$ (where it is not the case that $a = b = c$) is said to form a three-term arithmetic progression if $a + b = 2c$.
- We say that B is progression-free (or, equivalently, sum-free) if it does not contain three-term arithmetic progressions.

Question: what is the largest size that a progression-free subset can have?

Roth's Result

In 1952 and 1953, Klaus Friedrich Roth (who would later receive a Fields Medal for the Thue – Siegel – Roth theorem) estimated the largest possible size of a progression-free subset in $\{1, 2, \dots, N\}$. He published his results in the paper, "On Certain Sets of Integers".

- Roth discovered that a progression-free set $A \subset \{1, 2, \dots, N\}$ has size $O(N/\text{loglog}(N))$ as $N \to \infty$.
- His method used the Hardy-Littlewood Circle Method and tools from Fourier analysis.

The work of Roth inspired estimates for the size of progression-free subsets in other abelian groups.

The $\mathbb{Z}_4^n$ Case

In the years following Roth's result, a large amount of attention has been given to estimating the size of progression-free sets in subsets of powers of abelian groups. In the case of $\mathbb{Z}_4^n$:

- In 2011, Tom Sanders proved that the largest size that any progression-free subset of $\mathbb{Z}_4^n$ is $O(4^n/n(\log n)^\epsilon)$, where ϵ is a positive absolute constant.
- In 2016, Ernie Croot, Vsevolod Lev, and Peter Pal Pach showed that any progressions-free subset of $\mathbb{Z}_4^n$ has size smaller than $4^{\gamma n}$, where $\gamma \approx 0.926$.

The $\mathbb{F}_3^n$ Case

An even greater focus has been given to estimating the size of progression-free sets in $\mathbb{F}_3^n$. In this case, a triple of elements a, b, c (where it is not the case that $a = b = c$) forms a three-term arithmetic progression if $a + b + c = 0$, so our problem is equivalent to finding the largest set whose elements do not form a line.

- In 1995, Roy Meshulam modified Roth's proof to show that the largest size of any progression-free set in $\mathbb{F}_3^n$ is $O(3^n/n)$.
- In 2012, Michael Bateman and Nets Hawk Katz improved this result; they discovered that $O(3^n/n^{1+\epsilon})$, where where ϵ is a positive absolute constant, is a better estimate.
- In 2016, Jordan Ellenberg and Dion Gijswijt proved that any progression-free set in $\mathbb{F}_q^n$ has a size bounded above by c^n, where $c < q$. In particular, $|A| = o(2.756...^n)$ for any progression-free set A in $\mathbb{F}_3^n$. Robert Kleinberg, William Sawin, and David Speyer wrote a conjecture that this bound is quite sharp, which Luke Pebody lated proved.

The Importance of the Results from 2016

The results from the Croot-Lev-Pach paper "Progression-Free Sets in $\mathbb{Z}_4^n$ are Exponentially Small" and the Ellenberg-Gijswijt paper "On Large Subsets of $\mathbb{F}_q^n$ with no Three-Term Arithmetic Progression" received a large amount of attention. Why?

- For the first time, bounds were obtained that are exponential rather than logarithmic.
- The Croot-Lev-Pach paper uses a polynomial method of proof rather than Roth's Fourier analysis-focused method. The Ellenberg-Gijswijt paper also uses this polynomial method, but for a stronger result.

In my thesis, I generalize results from both of these papers to find bounds for the size of progression-free subsets in non-abelian groups.

The Ellenberg-Gijswijt Method (1/2)

A summary of the Ellenberg-Gijswijt method follows. I omit proofs, as I later provide proofs to my own generalizations of these results. Ellenberg and Gijswijt begin by generalizing Lemma 1 from the Croot-Lev-Pach paper. For comparison:

- **Lemma 1 (C-L-P).** Suppose that $n \geq 1$ and $d \geq 0$ are integers, P is a multilinear polynomial in n variables of total degree at most d over a field $\mathbb{F}$, and $A \subseteq \mathbb{F}^n$ is a set with $|A| > 2\sum_{0 \leq i \leq d/2} \binom{n}{i}$. If $P(a-b) = 0$ for all $a, b \in A$ with $a \neq b$, then also $P(0) = 0$.
- **Proposition 2 (E-G).** Let $\mathbb{F}_q$ be a finite field and let A be a subset of $\mathbb{F}_q^n$. Let α, β, γ be three elements of $\mathbb{F}_q$ which sum to 0. Suppose $P \in S_n^d$ satisfies $P(\alpha a + \beta b) = 0$ for every pair a, b of distinct elements of A. Then the number of $a \in A$ for which $P(-\gamma a) \neq 0$ is at most $2m_{d/2}$.

Here, m_d is the size of the set monomials in n-variables having degree in each variable at most $q-1$ and total degree at most d. By multilinear, we mean linearity in each variable.

The Ellenberg-Gijswijt Method (2/2)

Next, a generalized upper bound is found:

- **Theorem 4 (E-G).** Let α, β, γ be elements of $\mathbb{F}_q$ such that $\alpha + \beta + \gamma = 0$ and $\gamma \neq 0$, and let A be a subset of $\mathbb{F}_q^n$ such that the equation $\alpha a_1 + \beta a_2 + \gamma a_3 = 0$ has no solutions $(a_1, a_2, a_3) \in A^3$ apart from those with $a_1 = a_2 = a_3$. Then $|A| \leq 3m_{(q-1)n/3}$.

Theorem 4 is then used to estimate the size of a progression-free subset:

- **Corollary 5 (E-G).** Let A be a subset of $(Z/3Z)^n$ containing no three-term arithmetic progression. Then $|A| = o(2.756^n)$.

How the C-L-P Method Relates to the Non-Abelian Case

While Lemma 1 from the paper by Croot, Lev, and Pach works for $\mathbb{F}_q^n$, their final result is for $\mathbb{Z}_4^n$, and $\mathbb{Z}_4$ is not a field. They are able to obtain their bound by noting that $\mathbb{Z}_2$ is an ideal of $\mathbb{Z}_4$ which is a field, and then apply Lemma 1 to the cosets of this field:

- In the $\mathbb{Z}_4^n$ case, we have that $\mathbb{Z}_2 \hookrightarrow \mathbb{Z}_4 \to \mathbb{Z}_2$, so the result is applied for the 2^n cosets of $\mathbb{Z}_2^n$ in $\mathbb{Z}_4^n$.

We use a similar method for non-abelian groups, in which apply the result to cosets of normal subgroups which are isomorphic to fields in their parent groups.

The Non-Abelian Case

A definition of a progression-free set in the non-abelian case:

- Let A be a non-abelian group and let B be a subset of A. A triple of elements $a, b, c \in B$ (where it is not the case that $a = b = c$) is said to form a three-term arithmetic progression if $ab = c^2$. We say that B is progression-free if it does not contain three-term arithmetic progressions.

We use S_3^n as the main example for finding bounds in the non-abelian case:

- $A_3^n(\simeq \mathbb{Z}_3^n) \leq S_3^n \to \mathbb{Z}_2^n$.

Examples

We provide basic examples to demonstrate the concept of a progression-free set in S_3:

- $\{(\,), (123)\}$ is a progression free set in S_3. Note that $(\,)^2 = (\,), (123)^2 = (132), (\,)(123) = (123)$, and $(123)(\,) = (123)$, so we cannot choose a, b, c (not all equal) such that $ab = c^2$.
- However, $\{(), (12)\}$ is not progresson-free in S_3, since $(\,)(\,) = (12)^2$.

We now modify the relevant results from C-L-P and E-G to work for non-abelian groups.

The S_3^n Case (1/9)

We begin with Lemma 1 from C-L-P/Proposition 2 from E-G. Here, $\cdot$ represents componentwise multiplication of vectors (if $r = (r_1, \dots r_n)$ and $s = (s_1, \dots s_n)$, then $r \cdot s = (r_1 s_1, \dots, r_n s_n)$).

Proposition 2 (E-G), Modified. Let $A \subset \mathbb{Z}_3^n$. Let $\alpha, \beta, \gamma \in \mathbb{Z}_3^n$ such that $\alpha + \beta = 2\gamma$. Let K_n^d be the span of the set of monomials having degree in each variable at most 2 and total degree at most d, and suppose $P \in K_n^d$ satisfies $P(\alpha \cdot a + \beta \cdot b) = 0$ for every pair a, b of distinct elements of A. Then the number of $c \in A$ for which $P(-\gamma c) \neq 0$ is at most $2m_{d/2}$.

Proof. Since $P \in K_n^d$ we can rewrite $P(\alpha \cdot a + \beta \cdot b)$ as

$$\sum_{deg(m)+deg(m')\leq d} C_{m,m'} m(a)m'(b),$$

where m, m' are monomials in n-variables having degree in each variable at most 2 and total degree at most d, and $C_{m,m'}$ is a constant depending on m and m'.

The S_3^n Case (2/9)

Note that at least of one m, m' in each summand must have degree at most $d/2$, so we can further rewrite this as

$$\sum_{deg(m)\leq d/2} m(a)F_m(b) + \sum_{deg(m)\leq d/2} m(b)G_m(a),$$

where F_m, G_m are polynomials depending on m.

Now, define M to be the $|A|$ by $|A|$ matrix so that $M_{ab} = P(\alpha \cdot a + \beta \cdot b)$. Then M is the sum of $2m_{d/2}$ rank one matrices, so its rank is at most $2m_{d/2}$. However, note that M must be a diagonal matrix, so we have that no more than $2m_{d/2}$ diagonal elements of M are nonzero. This implies the result. $\square$

This proof works for subsets of any coset of $\mathbb{Z}_3^n$ in S_3^n as well, as multiplication of elements in each coset is linear. We choose α, β, and γ differently depending on the coset.

The S_3^n Case (3/9)

$\cdot$	()	(1 2 3)	(1 3 2)
()	()	(1 2 3)	(1 3 2)
(1 2 3)	(1 2 3)	(1 3 2)	()
(1 3 2)	(1 3 2)	()	(1 2 3)

Table: Multiplication in A_3. Using the relations $0 = ()$, $1 = (123)$, $2 = (132)$, we see that ab becomes $a + b$, and thus c^2 becomes $2c$.

$\cdot$	(1 2)	(1 3)	(2 3)
(1 2)	()	(1 3 2)	(1 2 3)
(1 3)	(1 2 3)	()	(1 3 2)
(2 3)	(1 3 2)	(1 2 3)	()

Table: Multiplication in the complement of A_3. Using the relations $0 = (12), 1 = (13), 2 = (23)$, along with the relations from the previous coset for products, we see that ab becomes $a - b$, and thus c^2 becomes 0.

The S_3^n Case (4/9)

In this example, I show how we would calculate α, β, γ for S_3^2.

Note that $S_3^2/\mathbb{Z}_3^2 \simeq \mathbb{Z}_2^n$, so each of the four cosets of $\mathbb{Z}_3^2$ corresponds to one of $\begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix} \in \mathbb{Z}_2^2$.

Fixing $\alpha = \begin{pmatrix}1\\1\end{pmatrix}$, we can set β as each of the four coset vectors and find γ using $\alpha + \beta = -\gamma$.

For one coset, we have $\alpha = \begin{pmatrix}1\\1\end{pmatrix}, \beta = \begin{pmatrix}0\\0\end{pmatrix}, \gamma = \begin{pmatrix}-1\\-1\end{pmatrix}$.

For the next coset, we have $\alpha = \begin{pmatrix}1\\1\end{pmatrix}, \beta = \begin{pmatrix}0\\1\end{pmatrix}, \gamma = \begin{pmatrix}-1\\-2\end{pmatrix}$.

For the next coset, we have $\alpha = \begin{pmatrix}1\\1\end{pmatrix}, \beta = \begin{pmatrix}1\\0\end{pmatrix}, \gamma = \begin{pmatrix}-2\\-1\end{pmatrix}$.

For the final coset, we have $\alpha = \begin{pmatrix}1\\1\end{pmatrix}, \beta = \begin{pmatrix}1\\1\end{pmatrix}, \gamma = \begin{pmatrix}-2\\-2\end{pmatrix}$.

The S_3^n Case (5/9)

Next, we modify Theorem 4 from the E-G paper:

Theorem 4 (E-G), Modified. Let A be progression-free in S_3^n. For $v \in \mathbb{Z}_2^n (\simeq S_3^n / A_3^n)$, let Av denote the intersection of A with the coset of $\mathbb{Z}_3^n$ in S_3^n corresponding to v. Then $|Av| \leq 3m_{2n/3}$.

Proof. Consider $-\alpha \cdot Av$. Note that its complement in $\mathbb{Z}_3^n v$ has size $3^n - |Av|$.

Define V to be the set of polynomials that are zero on $(-\alpha \cdot Av)^c$, where the superscript c denotes complement, and let K_n^d be the span of the set of monomials having degree in each variable at most 2 and total degree at most d.

Then V is the kernel of a mapping ϕ from K_n^d to the set of functions on $(-\alpha \cdot Av)^c$, so by the rank-nullity theorem, we have that dim $V =$ dim $K_n^d -$ dim(Im $\phi) \geq m_d - 3^n + |Av|$.

The S_3^n Case (6/9)

Define $S(A) := \{\beta \cdot b + \gamma \cdot c | b \neq c\}$. Note that $S(A)$ is disjoint from $(-\alpha \cdot Av)^c$, so that any element of V vanishes on $S(A)$. From the modified Proposition 2, we have for any $P \in V, P(-\alpha \cdot z) \neq 0$ for at most $2m_{d/2}$ points z of Av.

Let $R \in V$ have maximal support and let Σ be the support of R. Note that $|\Sigma| \geq \dim V$, since if not, there would exist a nonzero $S \in V$ vanishing on Σ. However, then the support of $R + S$ would strictly contain Σ, contradicting R having maximal support.

Note that any element of V has its support contained in $-\alpha \cdot Av$, so $\dim V \leq |\Sigma| \leq 2m_{d/2}$. Thus, $2m_{d/2} \geq m_d - 3^n + |Av|$. We rewrite this as $|Av| \leq 2m_{d/2} - m_d + 3^n$.

There are $3^n - m_d$ monomials having individual degree less than 3 and total degree greater than d. These are in bijection with monomials whose degree is less than $2n - d$, of which there are at most m_{2n-d}. Thus, $3^n - m_d \leq m_{2n-d}$, so we can take $d = 2n/3$ to get the result.

The S_3^n Case (7/9)

We can easily generalize the results from Lemma 4:

Theorem 4 (E-G), Generalized. Let G be a non-abelian group. Let A be a progression-free set in G^n. Let H^n be a normal subgroup of G^n isomorphic to $\mathbb{F}_q^n$ in G^n. Define Av as before (this time with $v \in (G/H)^n$). Then we have that $|Av| \leq 3m_{(q-1)n/3}$.

Proof. Nearly identical. Let K_n^d be the span of the set of monomials having degree in each variable at most $q-1$ and total degree at most d (here, d is an integer in [0, (q-1)n]). Defining V and $S(A)$ as before, we have that $\dim V \geq m_d - q^n + |Av|$ and $\dim V \leq 2m_{d/2}$. Thus, $2m_{d/2} \geq m_d - q^n + |Av|$. Noting that $q^n - m_d \leq m_{(q-1)n-d}$, we can take $d = (q-1)n/3$ to get the result. $\square$

The S_3^n Case (8/9)

Corollary 5 from E-G depends on the following information to bound $m_{(q-1)n/3}$:

For fixed q, $m_{(q-1)n/3}/q^n$ becomes exponentially smaller as we increase n. One can define a random variable X with values $0, 1, \ldots, q-1$ each occurring with a probability of $1/q$. Then $m_{(q-1)n/3}/q^n$ is the probability that n independent copies of X have mean at most $(q-1)/3$.

Let $J(\theta, x, q) = \theta x - log((1 + e^{\theta} + \ldots + e^{(q-1)\theta})/q)$. By Cramer's Theorem, $\lim_{n\to\infty}(1/n)(log(m_{(q-1)n/3}/q^n)) = -I((q-1)/3)$, where $I(x)$ is the supremum of $J(\theta, x, q)$ when varying θ.

Note that $I(x)$ is positive, as $J(\theta, x, q)$ takes value 0 at $\theta = 0$ and has nonzero derivative at $\theta = 0$ except when $x = (q-1)/2$. Thus, the supremum of $J(\theta, x, q)$ is positive, so $m_{(q-1)n/3} = O(c^n)$ for some $c < q$.

The S_3^n Case (9/9)

Corollary 5 (E-G). Let A be a subset of $(Z/3Z)^n$ free of three-term arithmetic progressions. Then $|A| = o(2.756^n)$.

Proof. Let $q = 3$, so $x = 2/3$. Note that $I(2/3)$ is attained when $e^\theta = (\sqrt{33} - 1)/8$. Thus, we get the bound $3e^{-I(2/3)} < 2.756$. Theorem 4 implies the result. $\square$

We modify this result to find a bound for the S_3^n case:

Corollary 5 (E-G) Modified. Let A be a subset of S_3^n free of three-term arithmetic progressions. Then $|A| = o(5.512^n)$.

Proof. We look at $\mathbb{Z}_3^n$ in S_3^n. Let $q = 3$, so $x = 2/3$. from the original proof, we get the bound $3e^{-I(2/3)} < 2.756$ for any coset Av. There are 2^n choices for v, so $|A| = o(5.512^n)$. $\square$

Other Non-Abelian Groups

We can view the E-G bound for $\mathbb{F}_q^n$ as "gamma value" γ_q. Using these gamma values, we can find bounds for progression-free set in the non-abelian case using the following formula:

Corollary 5 (E-G) Generalized. Let G be a non-abelian group. Let H be a normal subgroup of G isomorphic to a $\mathbb{F}_q$. Let k be the number of cosets of H in G. Let A be a progression-free set in G^n. Then $|A| \leq k^n \gamma_q^n$.

Proof. γ_q^n is the bound for progression-free sets in each coset. Since there are k^n cosets, the result follows. □

Examples

Repeating this process for other groups yields the following bounds:

Theorem. Let A be a subset of $(D_{10})^n$ (Here, D_{10} is the dihedral group of order 10) free of three-term arithmetic progressions. Then $|A| = o(8.9232^n)$.

Theorem. Let A be a subset of $(Q_8)^n$ (Q_8 is the quaternion group) free of three-term arithmetic progressions. Then $|A| = o(7.2200^n)$.

Theorem. Let A be a subset of $\mathrm{Aff}(\mathbb{F}_4)^n$ (affine group) free of three-term arithmetic progressions. Then $|A| = o(10.8303^n)$.

Theorem. Let A be a subset of $\mathrm{Aff}(\mathbb{F}_5)^n$ free of three-term arithmetic progressions. Then $|A| = o(17.8464^n)$.

In the examples involving affine groups, we use the group of translations as our normal subgroup. This results in a non-cyclic quotient group ($\simeq GL_n(\mathbb{F}_q)$), for which our method still works.

Other Results (1/2)

Remark. Let G be a non-abelian group and H be a normal subgroup of G. Let $C_1, \dots C_m$ be the cosets of H in G. If D_i is a progression-free set in C_i for all $i \in \{0, \dots, m\}$, it is not necessarily the case that $D_1 \bigcup \dots \bigcup D_m$ is a progression-free set in G.

Proof. Consider $G = S_3^n$, $H = A_3^n$. Let B be the complement of A_3 in S_3. Note that A_3^n and B^n are both cosets of A_3^n in S_3^n. Note also that $\left\{ \Big((\,), \dots, (\,) \Big), \Big((\,), \dots, (\,), (123) \Big) \right\}$ is a progression-free set in A_3^n, and $\left\{ \Big((12), \dots, (12) \Big) \right\}$ is a progression-free set in B^n. However, note that $\Big((\,), \dots, (\,) \Big) \Big((\,), \dots, (\,) \Big) = \Big((12), \dots, (12) \Big)^2$, so their union is not progression-free in S_3^n. $\square$

The above result tells us that our upper bound using gamma values has room for improvement.

Other Results (2/2)

Trivially, we have that γ_q^n is a lower bound for the maximum size of a progression-free set (where the normal subgroup is isomorphic to $\mathbb{F}_q^n$). We improve this bound for the case when our original group is the direct sum of fields:

Theorem. Suppose a group G is the direct product of fields A, B, where $|A| = s$ and $|B| = t$. The maximal size of a progression-free set in G^n is greater than $(\gamma_s \gamma_t)^n$.

Proof. Let S_1 be a progression-free set in A^n, and S_2 be a progression-free set in B^n. Claim: $S_1 \oplus S_2$ is progression-free in G^n. Suppose for contradiction that $(a_1, a_2) + (b_1, b_2) = 2(c_1, c_2)$ is a progression in $S_1 \oplus S_2$, where $(a_1, a_2), (b_1, b_2), (c_1, c_2) \in S_1 \oplus S_2$. Since S_1 and S_2 are progression-free, we have that $a_1 + b_1 = 2c_1$ implies that $a_1 = b_1 = c_1$, and $a_2 + b_2 = 2c_2$ implies that $a_2 = b_2 = c_2$. Thus, $(a_1, a_2) = (b_1, b_2) = (c_1, c_2)$, so $(a_1, a_2), (b_1, b_2), and (c_1, c_2)$ do not form a progression-free set in $S_1 \oplus S_2$. Since $S_1 \oplus S_2$ is progression-free, we have that G^n has size greater than $(\gamma_s \gamma_t)^n$. $\square$