

7. NOTES ON AN INVERSE THEOREM (BY ANINDYA C. PATTHAK)

- (1) Finite field philosophy : translate questions regarding $\mathbb{Z}/N\mathbb{Z}$ over finite fields.
for eg., What is the largest value of $|A|$ (where $A \subseteq [N]$) with no solutions $x + z = 2y$.
- (2) Offers linear algebraic technique
- (3) Bourgain's observation : some generic machinery to convert arguments on the finite field setting to arguments which work for arbitrary group G by using a kind of an "approximate linear algebra".

We will assume knowledge of basic fourier transform over an arbitrary abelian group.

7.1. Roth's proof : A step into uniformity. Consider $A \subseteq \mathbb{Z}/N\mathbb{Z}$ of density δ (i.e., $|A| = \delta N$). We are interested in length three AP in A . For a set A , by abusing notation, we denote its characteristic function by A .

Now let $A, B, C \subseteq \mathbb{Z}/N\mathbb{Z}$. Then

$$\begin{aligned} \mathbb{E}_{x,d} A(x)B(x+d)C(x+2d) &= N^{-2} \sum_{x,d} \sum_{rst} \hat{A}(r)\hat{B}(s)\hat{C}(t)w^{-r \cdot x}w^{-s \cdot (x+d)}w^{-t \cdot (x+2d)} \\ &= N^{-1} \sum_x \sum_{rs} \hat{A}(r)\hat{B}(-2s)\hat{C}(s)w^{-x \cdot (r-s)} \\ &= \sum_r \hat{A}(r)\hat{B}(-2r)\hat{C}(r). \end{aligned}$$

If $\max_r \hat{C}(r) \leq \gamma N$ (and assume $|A| = |B|$) then note that the above is bounded by $\gamma N \|\hat{A}\|_2 \|\hat{B}\|_2 = \gamma N^2 |B|$. In that case, we say that the set C is γ -uniform.

Roughly the proof (roughly) follows in two cases : If the set is γ -uniform for a suitable γ , then set $B = A \cap [N/3, 2N/3]$. Then it is shown that exists $(x, y, z) \in A \times B^2$ which is a genuine progression. On the other hand, if the set is not γ -uniform, then it has large fourier component, and then some work is needed to come up with a with a genuine arithmetic progression P of size roughly $\Omega(N^{1/2})$ such that $\frac{|A \cap P|}{|P|} \geq \delta + \epsilon$ for some $\epsilon > 0$. For more details see [2].

7.2. Gowers generalization. We first define convolution. Let $f, g : \mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{C}$ be two function then

$$f * g(x) \stackrel{\text{def}}{=} \sum_y f(y)\overline{g(x+y)}.$$

We now record a lemma which kind of paves way to the generalization of uniformity to the higher order.

Lemma 7.1. *Let f be a function $f : \mathbb{Z}_N \rightarrow D \subseteq \mathbb{C}$ (D denotes the unit disc). Then the following are equivalent.*

- (1) f is α -uniform i.e., $\max_r |\hat{f}(r)| \leq \alpha N$.
- (2) $\sum_r |\hat{f}(r)|^4 \leq c_1 N^4$, where $c_1 \leq \alpha^2 \leq c_1^{1/2}$.
- (3) $\sum_k |\sum_s f(s)\overline{f(s-k)}|^2 \leq c_1 N^3$.

Proof. Straightforward. (Or see [1].) □

Now observe that

$$\begin{aligned} \sum_k \left| \sum_s f(s) \overline{f(s-k)} \right|^2 &= \sum_k \sum_{st} f(s) \overline{f(s-k)} \overline{f(t)} f(t-k) \\ &= \sum_u \sum_{sv} f(s) \overline{f(s-u)} \overline{f(s-v)} f(s-u-v) \end{aligned}$$

It turns out that this definition (of pseudorandom set) is not strong enough to prove Szemerédi's theorem for AP of length 4. This is because an α -uniform set need not contain roughly the expected number of length four AP. However, the definition that works is the following.

A function $f : \mathbb{Z}_N \rightarrow D$ is said to be quadratically α -uniform if

$$\sum_{u,v} \left| \sum_s f(s) \overline{f(s-u)} \overline{f(s-v)} f(s-u-v) \right|^2 \leq \alpha N^4,$$

which can be put into

$$\mathbb{E}_{x, y_1, y_2, y_3} \left(\prod_{S \subseteq [3]} C^{|S|} f\left(x + \sum_{i \in S} y_i\right) \right) \leq \alpha$$

where C is the conjugation operator, which is also known as the (eighth power of) Gowers U^3 -norm.

In general for $d \geq 1$, Gowers U^d th norm is defined as

$$U^d(f) \stackrel{\text{def}}{=} \|f\|_{U^d}^{2^d} \stackrel{\text{def}}{=} \mathbb{E}_{x, y_1, \dots, y_d} \left[\prod_{S \subseteq [d]} C^{|S|} f\left(x + \sum_{i \in S} y_i\right) \right].$$

claim: If a set is quadratically α -uniform, then it is $\sqrt{\alpha}$ uniform.

Proof. Expanding (3) of Lemma 7.1, we get

$$\begin{aligned} \sum_k \sum_{st} |f(s) \overline{f(s-k)} \overline{f(t)} f(t-k)| &= \sum_k \sum_{su} |f(s) \overline{f(s-k)} \overline{f(s-u)} f(s-u-k)| \\ &= \sum_{uv} \left| \sum_s f(s) \overline{f(s-u)} \overline{f(s-v)} f(s-u-v) \right|. \end{aligned}$$

The Claim follows from Cauchy-Schwartz. \square

Remark. The above claim holds for any d and $d+1$ order uniformity, i.e., $(d+1)$ th order uniformity implies d th order uniformity. However, the reverse does not hold. Functions similar to Bent function can be shown to violate the reverse connection.

Proposition 7.2. (Inverse theorem for Gowers norm of order two) $U^2(f) \geq \alpha \implies \|\hat{f}\|_\infty \geq \sqrt{\alpha}$.

Proof. Immediate from Lemma 7.1. \square

7.3. Inverse theorem for Gowers norm of order three.

Question 7.3. Suppose $U^3(f) \geq \delta$, what can we say about f ?

Proposition 7.4. ([3]) (Inverse theorem for U^3 norm over \mathbb{F}_5^n) Suppose that $f : \mathbb{F}_5^n \rightarrow [-1, 1]$ is a function for which $U^3(f) \geq \delta$. Then there exists a matrix $M \in \mathbb{F}_5^{n \times n}$ and a vector r so that

$$|\mathbb{E}_x f(x) w^{(x, Mx+r)}| \geq \Omega(1).$$

([4]) (Inverse theorem for U^3 norm over \mathbb{F}_2^n) Suppose that $f : \mathbb{F}_2^n \rightarrow [-1, 1]$ is a function for which $U^3(f) \geq \delta$. Then there exists a quadratic function g such that

$$\text{dist}(f, g) \leq \frac{1}{2} - \epsilon'.$$

7.4. Inverse theorem over \mathbb{F}_2 . We now on follow [4]. Assume that f is a perfect degree two polynomial i.e., $f(x) = (-1)^{\langle Ax, x \rangle + a}$ for some binary matrix and a constant $a \in \{0, 1\}$. Define

$$f_y(x) \stackrel{\text{def}}{=} f(x+y)f(x).$$

Then note that

$$f_y(x) = (-1)^{\langle By, x \rangle + a'}$$

where $B = A + A^t$ is a zero-diagonal symmetric matrix. In particular this implies that $\hat{f}_y(By) = 1$ (for the moment, ignore the sign). Now if f is not a perfect two degree polynomial, still something like this holds which we now demonstrate.

Lemma 7.5. *Let B be a symmetric matrix with zero diagonal (i.e., symplectic) such that $\mathbb{E}_y \hat{f}_y^2(By) \geq \epsilon$, then there exists a quadratic polynomial g such that*

$$\|f - g\| \leq \frac{1}{2} - \epsilon'.$$

Proof. See [4]. □

Also we need to show that

Lemma 7.6. $U^3(f) \geq \delta \implies \mathbb{E}_y \hat{f}_y^2(By) \geq \epsilon$ for a symplectic matrix B .

We also need a quantitative analog of Balog-Szemerédi theorem. We follow Gowers [1, 2]. We begin with a combinatorial lemma.

Lemma 7.7. *Let X be a set of size m , and let A_1, \dots, A_n are subsets of X such that $\sum_{i,j \in [n]} |A_i \cap A_j| \geq \delta^2 mn^2$. Then there is a set $K \subseteq [n]$ of size at least $\delta^5 n / \sqrt{2}$, such that, for at least 16/17 fraction (or 90%) of the pairs of $(i, j) \in K^2$ $|A_i \cap A_j| \geq \delta^2 m / 2$.*

In particular, the result holds if $|A_i| \geq \delta m$ for all $i \in [n]$.

Proof. Let $B_i = \{j | i \in A_j\}$. Define $E_i = B_i^2$. For any given $x, y \in [n]$, We first calculate

$$p_{xy} \stackrel{\text{def}}{=} \Pr_{i \in [m]} [(x, y) \in E_i] = \frac{|A_x \cap A_y|}{m}.$$

Now choose independently and uniformly randomly j_1, \dots, j_5 and set

$$X = \cap_{k \in [5]} E_{j_k}.$$

Clearly, $\Pr[(x, y) \in X] = p_{xy}^5$. Thus

$$\mathbb{E}X = \sum_{xy} p_{xy}^5.$$

However, since $\sum_{xy} p_{xy} \geq \delta^2 n^2$, and since $\left(\frac{\sum p_{xy}}{n^2}\right)^5 \leq \left(\frac{\sum p_{xy}^5}{n^2}\right)$, we obtain $\mathbb{E}X \geq \delta^{10} n^2$. For the random choice of X , consider the subset $Y \stackrel{\text{def}}{=} \{(i, j) \in X : |A_i \cap A_j| \leq \delta^2 m / 2\}$ (i.e., all (i, j) such that $p_{ij} \leq \delta^2 / 2$). Clearly then $\mathbb{E}Y \leq (\delta^2 / 2)^5 n^2$. Thus $\mathbb{E}|X - 16Y| \geq \delta^{10} n^2 / 2$.

Thus there exists a choice of j_r such that $|X| \geq 16|Y|$ and $EX \geq \delta^1 0n^2/2$. Set $K^2 = X$ (i.e., $K \stackrel{\text{def}}{=} \cap B_{j_r}$).

For the second statement, let $s_i = |B_i|$. Then note $\frac{\sum_i s_i^2}{m} \geq \left(\frac{\sum_i s_i}{m}\right)^2 \geq \left(\frac{\delta m \cdot n}{m}\right)^2 \geq \delta^2 n^2$. □

We are now ready to prove the Balog-Szemerédi theorem. Given a set $A \in \mathbb{Z}^D$, by abuse of notation by A we also mean its characteristic function. Then note that

$$A * A(x) = \sum_y A(y)A(x+y) = \#\{(w, z) \in A^2 : x = w - z\}$$

Furthermore, note that

$$\begin{aligned} \|A * A\|_2^2 &= \sum_x A * A(x)^2 \\ &= \sum_{xyz} A(y)A(z)A(x+y)A(x+z) \\ &= \sum_{\substack{u-y=w-z \\ (u,w,y,z) \in A^4}} 1 = \#\{(u, y, z, w) \in A^4 : u - y = w - z\} \end{aligned}$$

We now consider the following proposition. [This is the same as Theorem 5.2 from Week 5, and the above lemma is the one promised to be included in the appendix. –ed.]

Proposition 7.8. *Let A be a subset of \mathbb{Z}^D of size m such that $\|A * A\|_2^2 \geq c_0 m^3$. Then there exists a subset $A'' \subset A$ of size at least cm such that $|A'' - A''| \leq Cm$. Moreover, C and c depends only on c_0 .*

Proof. Let define $f(x) = A * A(x)$. Then clearly $\|f\|_1 = m^2$, $\|f\|_\infty \leq m$, $\|f\|_2^2 \geq c_0 m^3$. Thus by an simple averaging argument

$$|A_1 \stackrel{\text{def}}{=} \{x : f(x) \geq c_0 m/2\}| \geq c_0 m/2.$$

Now define a graph G on the vertices of A , where $y \sim z$ iff $y - z \in A_1$ (and so is $(z - y)$). Clearly the average degree of the graph is at least $c_0^2 m^2 / (4m) = (c_0^2/4)m$. Thus again by averaging argument, there exists a set of vertices $A_2 \subseteq A$ of size $n \geq (c_0^2/8)m$ such that each of them has degree at least $(c_0^2/8)m$. Denote $\delta \stackrel{\text{def}}{=} c_0^2/8$. Denote the elements of A_2 as a_1, \dots, a_n , and their immediate neighbors by N_1, \dots, N_n . Note that for each i , $|N_i| \geq \delta m$. Thus by the previous lemma there exists a set $K \subset [n]$ such that 90% of the indices of $(i, j) \in K^2$ it holds $|N_i \cap N_j| \geq \delta^2 m/2$. Note that $|K| \geq \delta^5 n / \sqrt{2}$.

We now define a graph H on the vertices set of K where the edges are $\{(i, j) : |N_i \cap N_j| \geq \delta^2 m/2\}$. By the lemma above, the average degree of this graph is at least $9/10$. Thus applying averaging argument once again we note that there is a set of size at least $4|K|/5$ such that each of them has average degree $4|K|/5$ in H . Call this set A'' , this is the set that has small difference set. To see this, note that let $a_i, a_j \in A''$. Then note that a_i and a_j has at least $3|K|/5$ common neighbors. For each common neighbor a_k , it holds that $|N_i \cap N_k| \geq \delta^2 m/2$. For each $b \in N_i \cap N_k$, from the definition of graph G , $a_i - b$ and $b - a_k$ are popular differences, say p and q , respectively. Furthermore, each such popular difference,

say p , can be written as $p_1 - p_2$ in $c_0m/2$ ways. Thus $a_i - a_k$ can be written as $(a_i - b) - (a_k - b) = (p_1 - p_2) - (q_1 - q_2)$ in $\delta^2m/2 \times (c_0m/2)^2$. Similarly $a_j - a_k$ can be written as $(r_1 - r_2) - (s_1 - s_2)$ in $\delta^2m/2 \times (c_0m/2)^2$. Thus $a_i - a_j$ can be written as $(p_1 - p_2) - (q_1 - q_2) - (r_1 - r_2) + (s_1 - s_2)$ in at least $3|K|/5 \cdot (\delta^2m/2 \times c_0^2m^2/4)^2$ i.e., $\frac{3}{5} \cdot \frac{\delta^9 c_0^4 m^7}{2^7}$ many ways. Thus $A'' - A''$ can not have more than Cm many distinct element, for some C . □

References.

- [1] W. T. Gowers. A new proof of Szemerédi's theorem for arithmetic progressions of length four. *GFAA (Geometric and Functional Analysis)*, 8, 1998.
- [2] W. T. Gowers. A new proof of Szemerédi's theorem. *GFAA (Geometric and Functional Analysis)*, 11(3):465–588, 2001.
- [3] B. Green and T. Tao. An inverse theorem for the Gowers U^3 norm. *math.NT/0503014*, 2005.
- [4] A. Samorodnitsky. Low-degree tests at large distance. In *ECCC report No 54*, 2006.