# Product-free sets and representations

Arithmetic Combinatorics (Fall 2016)
Rutgers University
Swastik Kopparty
Last modified: Sunday 18th December, 2016

Recall that a subset $A$ of a group $G$ is called product-free, if $ab \neq c$ for all $a, b, c \in A$.
Let $G$ be the group $PSL_2(\mathbb{F}_q)$. Let $n = |G|$. We now prove the very striking result of Gowers (see also the generalizations of Babai-Nikolov-Pyber) that if $A$ is a product-free set in $G$, then $|A| < n^{0.9}$. This is in sharp contrast to the abelian group case, where such $A$ exist with size $\Omega(|G|)$.
The only fact that we need about our group $G$, which we do not prove here, is:

- The dimension of every nontrivial irreducible representation of $G$ is $\Omega(n^{1/3})$.

## 1 Representation Theory

Let $\mathsf{Irrep}(G)$ denote the set of irreducible representations of $G$. Let $\rho_0 \in \mathsf{Irrep}(G)$ denote the trivial 1-dimensional representation.
Representation theory gives us a nice orthogonal basis for functions on $G$. For each $\rho \in \mathsf{Irrep}(G)$, we view $\rho$ as a homomorphism from $G$ to the group of complex $\dim(\rho)$-dimensional unitary matrices in $G$. Thus $\rho(g) \cdot \rho(h) = \rho(gh)$ for all $g, h \in G$. For each $i, j \in [\dim(\rho)]$, we get a function $\rho_{ij} : G \cdot \mathbb{C}$, such that $\rho_{ij}(g)$ equals the $i, j$ entry of the matrix $\rho(g)$.
We then have the basic orthogonality relations:

$$\langle \rho_{ij}, \rho'_{k\ell} \rangle = \begin{cases} 1/\dim(\rho) & \rho = \rho', i = k, j = \ell \\ 0 & \text{otherwise} \end{cases}$$

Furthermore, we have $\sum_{\rho \in \mathsf{Irrep}(G)} \dim(\rho)^2 = |G|$, and thus the $\rho_{ij}$ form an orthogonal basis for the space of all functions from $G$ to $\mathbb{C}$.
Given a function $f : G \to \mathbb{C}$, we define the Fourier coefficient of $f$ at the irreducible representation $\rho$ by the formula:

$$\hat{f}(\rho) = \mathbb{E}_{g \in G}[f(g)\rho(g^{-1})].$$

Thus $\hat{f}(\rho)$ is a matrix.
We then have the Fourier inversion formula:

$$f = \sum_{\rho \in \mathsf{Irrep}(G)} \dim(\rho) \sum_{i,j \in [\dim(\rho)]} (\hat{f}(\rho))_{i,j} \cdot \rho_{ij},$$

which expresses $f$ as a linear combination of the $\rho_{ij}$.
Define the norms:

$$\|f\|_p = \mathbb{E}_{g \in G}[|f(g)|^p]^{1/p}.$$

Using the inner product relations between the $\rho_{ij}$, we get the following Parseval formula:

$$\begin{aligned} \|f\|_2 = \mathbb{E}_{g \in G}[|f(g)|^2] &= \sum_{\rho \in \mathsf{Irrep}(G)} \dim(\rho) \sum_{i,j \in [\dim(\rho)]} |(\hat{f}(\rho)_{i,j}|^2 \\ &= \sum_{\rho \in \mathsf{Irrep}(G)} \dim(\rho) \|\hat{f}(\rho)\|^2_{Frob}. \end{aligned}$$

(Here $\|\cdot\|_{Frob}$ denotes the Frobenius norm of a matrix, which equals the square root of the sum of squares of absolute values of the entries).
Define the convolution of functions $f, f' : G \to \mathbb{C}$ by:

$$f \star f'(x) = \mathbb{E}_{y \in G} f(y) f'(y^{-1}x).$$

Another important property of Fourier transform is behavior under convolution. This is given by the following (very simple to prove) identity:

$$\widehat{f \star f'}(\rho) = \hat{f}(\rho) \cdot \hat{f'}(\rho).$$

# 2 Proof of the main theorem

Let $A \subseteq G$, with $|A| = \alpha|G|$. Let $1_A : G \to \mathbb{C}$ be the indicator function of $A$. Then $1_A \star 1_A$ is supported on $A \cdot A$. We will show that if $|A|$ is big, then $|A \cdot A|$ is huge; much bigger than $|G| - |A|$, which implies that $A \cdot A$ and $A$ must intersect.
Note that $\widehat{1_A}(\rho_0) = \alpha$. By Parseval applied to $1_A$,

$$\alpha = \alpha^2 + \sum_{\rho \neq \rho_0} \dim(\rho) \|\widehat{1_A}(\rho)\|^2_{Frob}.$$

Now we look at $1_A \star 1_A$. By Cauchy-Schwarz, its support can be lower bounded as follows:

$$|supp(1_A \star 1_A)| \geq |G| \cdot \frac{\|1_A \star 1_A\|_1^2}{\|1_A \star 1_A\|_2^2} = |G| \frac{\alpha^4}{\|1_A \star 1_A\|_2^2}.$$

It remains to give an upper bound on $\|1_A \star 1_A\|_2^2$.
By the relationship between Fourier transform and convolution, we have:

$$\widehat{1_A \star 1_A}(\rho) = (\widehat{1_A}(\rho))^2.$$

In particular,

$$\widehat{1_A \star 1_A}(\rho_0) = \alpha^2.$$

By Parseval, we have:

$$\|1_A \star 1_A\| = \alpha^4 + \sum_{\rho \neq \rho_0} \dim(\rho) \|(\widehat{1_A}(\rho))^2\|^2_{Frob}.$$

We will use the following simple inequality about Frobenius norms: For matrices $M, N$,

$$\|MN\|_{Frob} \leq \|M\|_{Frob} \|N\|_{Frob}.$$

(Proof: Let $M_i, N_j$ denote the $i$th row and $j$th column of matrices $M, N$ respectively. Then

$$\begin{aligned} \|MN\|^2_{Frob} &= \sum_{i,j} |\langle M_i, N_j \rangle|^2 \leq \sum_{i,j} \|M_i\|^2 \|N_j\|^2 \\ &= (\sum_i \|M_i\|^2)(\sum_j \|N_j\|^2) = \|M\|^2_{Frob} \|N\|^2_{Frob}, \end{aligned}$$

as desired.)
Thus:

$$\|1_A \star 1_A\| \leq \alpha^4 + \sum_{\rho \neq \rho_0} \dim(\rho) \|\widehat{1_A}(\rho)\|^4_{Frob}.$$

We bound the second term as follows:

$$\begin{aligned}
\sum_{\rho\neq\rho_0}\dim(\rho)\|\widehat{1_A}(\rho)\|_{Frob}^4 &\leq \left(\sum_{\rho\neq\rho_0}\dim(\rho)\|\widehat{1_A}(\rho)\|_{Frob}^2\right)\left(\max_{\rho\neq\rho_0}\|\widehat{1_A}(\rho)\|_{Frob}^2\right)\\
&= (\alpha-\alpha^2)\left(\max_{\rho\neq\rho_0}\|\widehat{1_A}(\rho)\|_{Frob}^2\right)\\
&\leq (\alpha-\alpha^2)\cdot\frac{\left(\sum_{\rho\neq\rho_0}\dim(\rho)\|\widehat{1_A}(\rho)\|_{Frob}^2\right)}{\min_{\rho\neq\rho_0}\dim(\rho)}\\
&\leq \frac{(\alpha-\alpha^2)^2}{\min_{\rho\neq\rho_0}\dim(\rho)}\\
&\leq O\left(\frac{(\alpha-\alpha^2)^2}{n^{1/3}}\right).
\end{aligned}$$

Putting everything together, we get:

$$\begin{aligned}
|A\cdot A| &\geq n\cdot\frac{\alpha^4}{\alpha^4+\frac{(\alpha-\alpha^2)^2}{n^{1/3}}}\\
&= n\cdot\frac{1}{1+\frac{(\frac{1}{\alpha}-1)^2}{n^{1/3}}}\\
&\leq n(1-\frac{\frac{1}{\alpha}-1}{n^{1/3}}).
\end{aligned}$$

Thus if $\alpha > n^{-0.1}$, then $|A\cdot A| > n(1-\alpha)$, completing the proof.