INTRODUCTION

DEV GUPTA, SOHAM SEN, AND VRINDA SHARMA

Abstract. We will introduce some motivating problems.

Brief

To begin with, combinatorics is "a branch of mathematics concerning the study of finite or countable discrete structures." Of course, this definition encompasses many more topics than we can discuss in a summer project. The topics mentioned in the handout are tentative and there is no real consensus as to what should be covered in a project like this one. We encourage mentees to come up with their own topics that they wish to explore. In a very broad sense, this project serves to illustrate a few computer science applications of combinatorics that seem interesting. Unlike enumerative combinatorics, which is concerned with counting problems - we will mostly focus on extremal and additive portions in this project.

Pre-requisites

The ability to read and understand mathematical proofs is required. Some familiarity with the basics of graph theory, group theory and analysis.[1]

1. Ramsey Theory for Graphs

We will use the Pigeonhole Principle to study both the quantitative and the qualitative aspects of Ramsey theory.

Definition 1.1. Given $s \in \mathbb{N}$, let $R(s)$ be the minimum $n \in \mathbb{N}$ such that every red-blue colouring of the edges of K_n contains a subgraph isomorphic to K_s the edges of which all have the same color (refered to as being monochromatic)

Theorem 1.2. *(Ramsey, 1930) For every $s \in \mathbb{N}$, $R(s)$ is finite.*

Definition 1.3. (Ramsey numbers) Given $s, t \in \mathbb{N}$, let $R(s,t)$ be the minimum $n \in \mathbb{N}$ such that every red-blue colouring of the edges of K_n contains either a red K_s or a blue K_t.

Theorem 1.4. *(Erdős–Szekeres, 1935) For every $s, t \in \mathbb{N}$, $R(s,t) \leq \binom{s+t-2}{s-1}$. In particular, $R(s) = O(\frac{4^s}{\sqrt{s}})$*

Lower bounds for Ramsey's theorem.

1.0.1. *A first idea: Dense K_s-free graphs.*

Theorem 1.5. *(Mantel, 1907) If G is K_3-free then $e(G) \leq e(K_{\lceil n/2 \rceil, \lfloor n/2 \rfloor})$*

2010 *Mathematics Subject Classification.* Primary 05Dxx, 11B25, 11N13, 28Dxx, 37Axx.

[1]We'll provide handouts for those less familiar with the pre-requisites or seeking a review.

1.0.2. *The right idea: random construction.* We want the same from the red and the blue graph (they should be K_s-free). Their roles are symmetric. Each edge has as much reason to be red than to be blue. Let us choose the color of each edge uniformly at random, independently from each other.

Theorem 1.6. *(Erdős, 1947)* $R(t,t) \geq (1-o(1))\frac{t}{e\sqrt{2}}2^{t/2}$.

1.0.3. *Improving the constant factor.* Using some alterations to the random construction, we can improve the Erdős lower bound by a constant factor of $\sqrt{2}$.

Theorem 1.7. $R(t,t) \geq (1-o(1))\frac{t}{e}2^{t/2}$.

Other topics. Hypergraph Ramsey theorem, Canonical Ramsey, Two-colorable Hypergraphs.

2. Szemerédi's Regularity Lemma

The high level intuitive meaning of the Regularity Lemma of Szemerédi is that every graph is made up of three parts: a structured part, a quasirandom part, and an error part. The size of the structured part, the quality of quasirandomness, and the size of the error all depend on a parameter $\epsilon > 0$ that can be chosen arbitrary small.

Lemma 2.1. *(Regularity Lemma (Szemerédi, 1975)). For every real* $\epsilon > 0$ *and positive integer* $m \in N$*, there exists an integer* $M = M(\epsilon, m)$ *such that every graph* $G = (V, E)$ *with at least* m *vertices has an* ϵ*-regular partition* $V = V_0 \cup V_1 \cup \cdots \cup V_k$ *where* $m \leq k \leq M$

3. Extremal Set Theory and the Linear Algebra Method

A sunflower (or Δ-system) with k petals and a core Y is a collection of sets $S_1, \ldots, S_k$ such that $S_i \cap S_j = Y$ for all $i \neq j$; the sets $S_i \setminus Y$ are petals, and we require that none of them is empty. A family of pairwise disjoint sets is a sunflower (with an empty core).

Lemma 3.1. *(Sunflower Lemma) Let* F *be family of sets each of cardinality* s*. If* $|F| > s!(k-1)^s$ *then* F *contains a sunflower with* k *petals.*

Conjecture (Erdős and Rado). Let $f(s,k)$ denote the least integer so that any s-uniform family of $f(s,k)$ sets contains a sunflower with k petals.For every fixed k there is a constant $C = C(k)$ such that $f(s,k) < C^s$.

Applications. Circuit Lower Bounds

3.1. Chains and Antichains.

Definition 3.2. A chain in a poset P is a subset $C \subseteq P$ such that any two of its points (say x, y) are comparable in the sense that either $x \leq y$ or $y \leq x$ (or both) hold. An antichain is a subset $A \subseteq P$ such that no two of its points are comparable.

Theorem 3.3. *(Dilworth) Suppose that the largest antichain in the poset* P *has size* r*. Then* P *can be partitioned into* r *chains.*

Theorem 3.4. *(Sperner) Let* $\mathcal{F}$ *be a family of subsets of an* n *element set. If* $\mathcal{F}$ *is an antichain then* $|\mathcal{F}| \leq \binom{n}{\lfloor n/2 \rfloor}$.

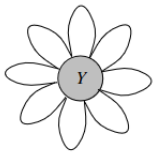

FIGURE 1. Sunflower with 8 petals and core Y

Theorem 3.5. *Given any poset of $mn+1$ elements, there exists either a chain of length $m+1$ or an anti-chain of length $n+1$.*

Theorem 3.6. *(Bollobás 1965) Let $A_1, \ldots, A_m$ and $B_1, \ldots, B_m$ be two sequences of sets such that $A_i \cap B_j = \phi$ if and only if $i = j$. Then, $\sum_{i=1}^{m} \binom{a_i+b_i}{a_i}^{-1} \leq 1$, where $a_i = |A_i|$ and $b_i = |B_i|$.*

Other topics. Union Free families

4. Expanders

4.1. **Ramanujan graphs.** Expander graphs can help to decrease the error-probability of Monte-Carlo randomized algorithms as well as to reduce the number of required random bits. We will show that using Ramanujan graphs the error probability can be reduced decently without any increase of the number of random bits. We will present yet another application of expander graphs to reduce the number of random bits.

4.2. **Connections to Extremal Number Theory.**

Theorem 4.1. *(Garaev 2007) Let p be a prime number, and $A \subseteq \mathbb{F}_p \setminus \{0\}$. Then the number of elements in at least one of the sets $A + A$ or $A \cdot A$ is at least an absolute constant times $min\{|A|^2/\sqrt{p}, \sqrt{p|A|}\}$. In particular, if $|A| \sim p^{2/3}$ then this minimum is about $|A|^{5/4}$.*

Expander codes. If $C \subseteq \{0,1\}^n$ is a linear code with a $k \times n$ generator matrix G, then the encoding of messages $w \in \{0,1\}^k$ is very easy: just encode w by the codeword $x = w^T G$. However, the decoding—that is, given a vector $y \in \{0,1\}^n$ find a codeword $x \in C$ closest to y - is in general linear codes a very difficult problem (it is "NP-hard"). We now show how using expander graphs one can construct linear codes for which decoding is almost trivial—it can be done in linear time! Moreover, if the expansion of the graph is good enough then the resulting codes achieve very good rate $(log_2|C|)/n$ and minimal distance.

4.3. **Expansion of random graphs.**

Theorem 4.2. *For every constant $d \geq 3$, there is a constant $\alpha > 0$ such that for all sufficiently large n, the graph $G_{n,d}$ is an $(\alpha, d-2)$ expander with probability at least 1/2.*

5. The Polynomail Method

Lemma 5.1. *(PIT lemma) Let $f(x_1, \ldots, x_n)$ be a nonzero polynomial of degree d over a field $\mathbb{F}$ and $S \subset F$ is a non-empty subset of the field elements. Then*

$Pr[f(r_1,\ldots,r_n)=0] \le d/|S|$ where $r_1,\ldots,r_n$ are random elements selected uniformly and independently from S.

Lemma 5.2. *(Kakeya conjecture in finite fields, Dvir 2009)*
Let $f \in \mathbb{F}[x_1,\ldots,x_n]$ be a polynomial of degree at most $q-1$ over a finite field with $q=|\mathbb{F}|$ elements. If f vanishes on a Kakeya set K, then f is the zero polynomial.

Theorem 5.3. *(Combinatorial Nullstellensatz) Let $f(x_1,\ldots,x_n)$ be a polynomial of degree d over a field $\mathbb{F}$. Suppose that the coefficient of the monomial $x_1^{t_1}\ldots x_n^{t_n}$ in f is nonzero and $t_1+\cdots+t_n=d$. If $S_1,\ldots,S_n$ are finite subsets of $\mathbb{F}$ with $|S_i| \ge t_i+1$, then there are exists a point x in $S_1\times\cdots\times S_n$ for which $f(x)=0$.*

Applications. Permanent lemma, Regular subgraphs, Sum-sets, Zero sum-sets

5.1. **The cap-set problem.** The cap set problem asks how large can a subset of $(\mathbb{Z}/p\mathbb{Z})^n$ be and contain no arithmetic progressions.

Theorem 5.4. *(Ellenberg-Gijswijt, 2016) For large d, $r_3(\mathbb{F}_3^d) < 2.76^d$*

5.1.1. *Fast Matrix Multiplication.* Let $w : n\times n$ matrices can be multiplied in $O(n^w)$ steps. Define $\omega = inf\{w\}$. Currently, the best algorithm known takes $O(n^{2.3729\ldots})$ steps, but it is conjectured that $\omega = 2$.

Definition 5.5. (Triple product property (TPP)) Given a group G, three subsets $S,T,U \subseteq G$ satisfy the triple product property if $s_{i'}^{-1}s_it_j^{-1}t_{j'}u_k^{-1}u_{k'} = 1 \iff i=i'$ and $j=j'$ and $k=k'$

Lemma 5.6. *(Blasiak, Church, Cohn, Grochow, Nasland, Sawin, and Umans) One cannot show that $\omega = 2$ using simultaneous TPP constructions in families of abelian groups of bounded exponent.*

6. Discrete Fourier Analysis

A central role in additive combinatorics is played by Bogolyubov's lemma and its variants, which shows that iterated sumsets of dense subsets of Abelian groups have considerable structure.

Definition 6.1. Let G be a finite Abelian group, let $\chi_1,\ldots,\chi_k \in \hat{G}$ be characters on G, and let $\delta > 0$. The Bohr set $B(\chi_1,\ldots,\chi_k;\delta)$ is the set

$$\{x \in G : \chi_i(x) \in e([-\delta,\delta]), i=1,\ldots,k\}$$

Theorem 6.2. *(Bogolyubov's lemma) Let G be a finite Abelian group and let $A \subset G$ be a subset of density α. Then $2A-2A$ contains a Bohr set of width 1/4 and dimension at most α^{-2}.*

6.0.1. *What do Bohr sets look like?*

Lemma 6.3. *Let G be a finite Abelian group and let $B=B(K,\delta)$ be a Bohr set in G, where K is a set of characters of size k. Then $\mid B \mid \ge \delta^k \mid G \mid$.*

We will show that Bohr sets in $\mathbb{Z}_N$ for prime N contain long arithmetic progressions.

Lemma 6.4. *Let $K \subset \hat{\mathbb{Z}}_N$ be a set of size k, let $\delta > 0$ and let $B=B(K,\delta)$. Then B contains an arithmetic progression of length at least $2\lfloor \delta N^{1/k} \rfloor + 1$.*

Applications : Fourier analysis on the Boolean hypercube

7. Sum-Product Theorem

Theorem 7.1. *(Sum Product Theorem for $\mathbb{F} = \mathbb{R}$) For $\mathbb{F} = \mathbb{R}$, $\exists \epsilon > 0$ such that $\forall A \subset \mathbb{F}$ either:*

(1) $|A + A| \geq |A|^{1+\epsilon}$
(2) $|A \times A| \geq |A|^{1+\epsilon}$

The best ϵ known in the above theorem is $4/3$, but it is conjectured that it holds for $\epsilon = 2 - o(1)$.

Theorem 7.2. *(Sum Product Theorem for $\mathbb{F} = \mathbb{F}_p$)*
For $\mathbb{F} = \mathbb{F}_p$ for p prime, $\exists \epsilon > 0$ such that $\forall A \subset \mathbb{F}$ with $|A| \leq |\mathbb{F}|^{0.9}$, either:

(1) $|A + A| \geq |A|^{1+\epsilon}$
(2) $A \times A| \geq |A|^{1+\epsilon}$

The best known ϵ in the above theorem is .001, and it is known that ϵ cannot be larger than $3/2$.

Definition 7.3. ((S, ϵ)-Disperser). A function $f : \{0,1\}^n \mapsto \{0,1\}^m$ for which all $X \in S$ satisfies: $|f(X)| \geq (1 - \epsilon)2^m$ is an (S, ϵ)-disperser. That is, $f(X)$ is a distribution with large support.

Definition 7.4. ((S, ϵ)-Extractor) A function $f : \{0,1\}^n \mapsto \{0,1\}^m$ for which all $X \in S$ satisfies: $||f(x) - U_m||_1 \leq \epsilon$ is an (S, ϵ)-disperser. That is, $f(X)$ is ϵ-close to the uniform distribution.

Before the sum-product theorem, Erdős (using the probabilistic method) showed that there exists an optimal 2-source extractor for all $k \geq 2logn$ in proving the existence of Ramsey Graphs. Explicit constructions for such extractors were known only for $k \geq n/2$. Using the sum-product theorem, (slightly) better results are possible: We have an explicit optimal 2-source extractor for $k \geq .4999n$. We can also give an explicit 2-source disperser for $m = 1$ and $k \geq \delta n$ and an explicit 2-source disperser for $m = 1$ and $k \geq n^{\delta}$.

Other topics. Plűnnecke-Ruzsa lemma, Balog-Szemeredi-Gowers lemma.

8. Uniformity Norms

We will briefly introduce Szemeredi's theorem and give an idea of how to prove it for arithmetic progressions of length 4. However, instead of proving that result, we shall prove the following closely related result, which involves many of the same ideas but is technically cleaner.

Lemma 8.1. *For every $\delta > 0$ and every prime $p \geq 5$ there exists n such that for every subset $A \subset \mathbb{F}_p^n$ there exist $a, d \in \mathbb{F}_p^n$ with $d \neq 0$ such that all of $a, a + d, a + 2d$ and $a + 3d$ belong to A.*

8.1. Gowers' Uniformity Norms.

Lemma 8.2. *The quadratic surface $A = \{x \in \mathbb{F}_p^n \mid \sum_{i \leq n/2} x_i x_{n/2+i} = 0 \in \mathbb{F}_p\}$ is linearly uniform, but contains a $\Theta(\delta^3)$ fraction of all arithmetic progressions of length k (k-APs) of $\mathbb{F}_p^n$ for every $k \geq 3$, where $\delta \sim 1/p$ is the density of A.*

Definition 8.3. (Directional Derivative) For a function $f : \mathbb{F}_p^n \mapsto \mathbb{C}$ and a vector $y \in \mathbb{F}_p^n$, the derivative in direction y is the function $D_y f : \mathbb{F}_p^n \mapsto \mathbb{C}$ with $D_y f(x) = f(x)\overline{f(x+y)}$.

Definition 8.4. The degree-d Gowers uniformity norm $U^d(f)$ of a function $f : G \mapsto \mathbb{C}$ is defined as $U^d(f) := (\mathbb{E}_{x,y_1,\ldots,yd \leftarrow R^G} D_{y_1 \ldots y_d} f(x))^{1/2d}$. Here, G is a finite group.

Theorem 8.5. *(Inverse theorem for U^3) Suppose $f : \mathbb{F}_p^n \mapsto \mathbb{C}$ is a function that takes values whose magnitudes are bounded by 1 everywhere. Let ω denote a p-th root of unity. If $U^3(f) > \eta$, then there exists a subspace W of dimension at least $n - \eta^{-O(1)}$, and, for each coset $y+W$, a quadratic polynomial $q_y(x)$ over $\mathbb{F}_p$ defined on $y + W$, such that*

$$\mathbb{E}_{y \leftarrow R^{\mathbb{F}_p^n}} \mid \mathbb{E}_{x \leftarrow R^{y+W}} f(x)\omega^{q_y(x)} \mid = \Omega(\eta^{O(1)})$$

We won't prove this theorem. But assuming this theorem, we will be able to prove Szemeredi's theorem for $k = 4$. The aim will be to show that non-uniformity implies that the set has higher density on some affine subspace of low codimension.

Lemma 8.6. *Every k-uniform subset of $\mathbb{F}_p^n$ is k-pseudorandom.*

Theorem 8.7. *Let $A \subseteq \mathbb{F}_p^n$ be set of density δ. If $U^3(\mathbf{1}_A - \delta) > \eta$ then there exists an affine subspace of dimension at least $n/2 - \eta^{-O(1)}$ on which A has density $\delta + \Omega(\eta^{O(1)})$.*

Using lemma 8.6 and theorem 8.7, we will prove Szemeredi's theorem for the groups $\mathbb{F}_p^n$ and $k = 4$ with simple induction.

8.1.1. *Direct Product Theorems.* We will use Gowers Uniformity to obtain XOR lemmas for correlation with low degree $\mathbb{F}_2$ polynomials.

Other topics. Probabilistically Checkable Proofs Constructions

9. Ergodic Theory

The ergodic-theoretic techniques in additive combinatorics are the least understood by theoretical computer scientists. In last five decades, there has been a substantial progress in Number theory due to the application of dynamical techniques. This new approach resolved many longstanding conjectures, for instance, Green-Tao theorem on primes in arithmetic progression etc. Also simple and more elegant proofs of existing results are found as well.
This project is devoted to the dynamical proofs of the two famous theorems:

(1) Theorem of Hardy and Littlewood, on Diophantine approximation, which has been reproved using topological dynamics, and
(2) Szemeredí's theorem on Additive combinatorics, which has been reproved using Ergodic theory

Definition 9.1. A dynamical system, in the simplest case, is a pair (X, T) comprising a nonempty set X and a map $T : X \longrightarrow X$. It can be regarded as the mathematical abstraction of a physical system with X as the ensemble of all possible states of the system that evolves according to the law T.

We are primarily concerned with following frameworks:

- **Topological dynamical system**: X is a compact metric space, and T is continuous.
- **Measure preserving system**: $(X, \mathcal{B}, \mu)$ is a measure space and T preserves μ, i.e., $\mu(T^{-1}(A)) = \mu(A)$, for all $A \in \mathcal{B}$.

9.1. **Recurrence in topological dynamics.**

Definition 9.2. Given a topological dynamical system (X, T), a point $x \in X$ is said to be *recurrent* if $\forall$ open $V \subseteq X$, $\exists n \in \mathbb{N}$ such that $T^n x \in V$, equivalently, $T^{n_k} x \xrightarrow[k\to\infty]{} x$, for some increasing sequence $\{n_k\}_{k\geq 1}$ of natural numbers.

Theorem 9.3. *Let K be a compact metric group and $a \in K$. Consider $R_a : K \to K$, $x \mapsto ax$. Then every point is recurrent.*

Definition 9.4. A morphism ϕ between two dynamical system (X, T) and (Y, S) is a continuous map $\phi : X \longrightarrow Y$ such that $S \circ \phi = \phi \circ T$. If ϕ is onto, then we call (Y, S) a *factor* of (X, T).

Definition 9.5. Let (Y, T_Y) be a dynamical system, K be a compact (metric) group and $\psi : Y \longrightarrow K$ be a continuous map. Let $X = Y \times K$ and $T_X(y, k) = (T_Y y, \psi(y)k)$. The system (X, T_X) is called *group extension* of (Y, T_Y).

Theorem 9.6. *If $y_0 \in Y$ is a recurrent point for T_Y, then $\forall k \in K$, (y_0, k) is a recurrent point for T_X.*

Theorem 9.7. ***Hardy-Littlewood, Weyl:*** *For $\alpha \in \mathbb{R}$ and $\varepsilon > 0$, we can solve the Diophantine inequality $\left|\alpha - \frac{m}{n^2}\right| < \frac{\varepsilon}{n^2}$, for $m, n \in \mathbb{Z}, n \neq 0$.*

9.2. **Recurrence in probability preserving systems.**

Definition 9.8. Let $(X, \mathcal{B}, \mu, T)$ be a measure preserving system. We say that it has *recurrence* property if one (or equivalently, all) of the following equivalent statements holds:

- $\forall A \in B$ with $\mu(A) > 0$, $\{x \in A : T^n x \in A \text{ for } \infty\text{-ly many } n\}$ is full.
- $\forall A \in B$ with $\mu(A) > 0$, $\mu(A \cap (\cup_{n\geq 1} T^{-n} A)) = \mu(A)$, i.e., for μ-a.e. $x \in A$, $T^n x \in A$, for some $n \in \mathbb{N}$.
- $\forall A \in B$ with $\mu(A) > 0$, there exists $n \in \mathbb{N}$ such that $\mu(A \cap T^{-n}(A)) > 0$.

Theorem 9.9. *Every probability preserving dynamical system has the recurrence property.*

Theorem 9.10. *Let (X, d) be a separable metric space, μ be a Borel probability measure, and $T : X \longrightarrow X$ preserve μ. Then $\mu-$ a.e. $x \in X$ is recurrent, i.e., $\lim_{k\to\infty} T^{n_k} x = x$, for an increasing sequence $\{n_k\}_{k\geq 1}$ in $\mathbb{N}$.*

Definition 9.11. Let $(X, \mathcal{B}, \mu, T)$ be a probability preserving system. Then it has MR property, i.e., $\forall A \in \mathcal{B}$ having $\mu(A) > 0$ and $k \geq 1$, $\exists n \in \mathbb{N}$ such that

$$\mu(A \cap T^{-n}(A) \cap T^{-2n}(A) \cap \cdots \cap T^{-kn}(A)) > 0.$$

9.3. **Background of Szemerédi's theorem.**

- van Dar Warden proved that if the integers are partitioned into finitely many subsets, one of them must possess arithmetic progressions of arbitrary finite length.
- Erdös and Turán made the following general conjecture in 1935:

Theorem 9.12. ***Erdös-Turán conjecture:*** *Let $A \subset \mathbb{Z}$ be a subset of the integers of* positive upper density*, i.e.,*

$$\limsup_{N\to\infty} \frac{1}{2N+1}\#([-N,N]\cap A) > 0. \tag{9.1}$$

Then, for all $k \geq 1$, A contains an arithmetic progression of length k.

- Note that, if $\mathbb{Z} = \bigsqcup_{1\leq i\leq k} A_i$, then one of the A_i's must have positive upper density. Hence the above conjecture implies van Dar Warden's theorem.
- K. Roth proved the above conjecture for $k = 3$.

Theorem 9.13. *Every p.p.s. has MR property if and only if Szemerédi's theorem holds.*

10. More Applications

10.1. Graphs with many disjoint triangles.

10.2. Impossibility of compression of NP-hard languages.

References

1. J. S. Ellenberg and D. Gijswijt *On large subsets of $\mathbb{F}_q^n$ with no three-term arithmetic progression*. Ann. of Math. (2) 185 (2017), no. 1, 339–343, DOI 10.4007/annals.2017.185.1.8. MR3583358
2. Sanjeev Arora and Boaz Barak. 2009. *Computational Complexity: A Modern Approach (1st. ed.)*. Cambridge University Press, USA. **p13**, 235–252
3. Ronald de Wolf. *A Brief Introduction to Fourier Analysis on the Boolean Cube*. Theory of Computing Library Graduate Surveys, TCGS 1 (2008), **pp**. 1–20
4. Jukna, S. (2001). *Extremal Combinatorics - With Applications in Computer Science*. Texts in Theoretical Computer Science. An EATCS Series. Springer.
5. Lovett, S. (2017). *Additive Combinatorics and its Applications in Theoretical Computer Science*. Number 8 in Graduate Surveys. Theory of Computing Library.
6. Tao, T. and V. H. Vu (2006). *Additive Combinatorics*. Cambridge Studies in Advanced Mathematics. Cambridge University Press.
7. H. Furstenberg, Y. Katznelson AND D. Ornstein (1982) *The Ergodic Theoretical Proof of Szemerédi's theorem*. BULLETIN (New Series) OF THE AMERICAN MATHEMATICAL SOCIETY Volume 7, Number 3.
8. H. Furstenberg (1981) *Recurrence in Ergodic Theory and Combinatorial Number Theory* . Princeton Legacy Library.
9. O'Donnell R. *Analysis of Boolean Functions*. Cambridge University Press; 2014.
10. Blasiak, Jonah, Thomas Church, Henry Cohn, Joshua A. Grochow, Eric Naslund, William F. Sawin, and Chris Umans. 2017. *On Cap Sets and the Group-Theoretic Approach to Matrix Multiplication*. Discrete Analysis
11. J Grochow. *The cap set conjecture and beyond*. BULLETIN (New Series) OF THE AMERICAN MATHEMATICAL SOCIETY Volume 56, Number 1, January 2019, Pages 29–64
12. A. Wigderson. *Applications of the sum-product theorem in finite fields* 21st Annual IEEE Conference on Computational Complexity (CCC'06), Prague, Czech Republic, 2006, pp. 1 pp. 111
13. Shlomo Hoory, Nati Linial and Avi Wigderson. *Expander graphs and their applications*. BULLETIN (New Series) OF THE AMERICAN MATHEMATICAL SOCIETY Volume 43, Number 4, October 2006, Pages 439–56.
14. W Gowers. 2017. *Generalizations of Fourier analysis, and how to apply them* American Mathematical Society BULLETIN (New Series) OF THE AMERICAN MATHEMATICAL SOCIETY Volume 54, Number 1, January 2017, Pages 1–44
15. Mini course on additive combinatorics, Princeton University, 2007 by Boaz Barak, Luca Trevisan and Avi Wigderson
16. Miscellaneous lecture notes, articles and blogs.