

# CS 2429 - Comm Complexity: Applications and New Directions

Lecturer: Lalla Mouatadid

## 1 Additive Combinatorics and Log Rank

Given any Boolean function  $f : \{0, 1\}^n \times \{0, 1\}^n \Rightarrow \{0, 1\}$ , it is well known that:

$$\log \text{rank}(M_f) \leq CC(f) \leq \text{rank}(M_f)$$

In [6], it was conjectured by Lovász and Saks that the upper bound is much tighter, namely that  $CC(f) = \log^{O(1)} \text{rank}(M_f)$ . This famous conjecture, known as the **Log Rank** conjecture is one of the biggest open questions in Communication Complexity. And until recently, the best known bounds in terms of the rank were:

$$\log \text{rank}^{\log_3 6}(M_f) \approx \log \text{rank}^{1.63}(M_f) \leq CC(f) \leq 0.415 \text{rank}(M_f)$$

where the lower bound is due to Kushilevitz [unpublished, 1995] and the upper bound due to Kotlov in [5].

In 2012, Ben Sasson, Lovett and Zewi gave a conditional improvement on the upper bound [2], namely  $O\left(\frac{\text{rank}(M_f)}{\log \text{rank}(M_f)}\right)$  assuming the well-known conjecture in Additive Combinatorics: The Polynomial Freiman-Ruzsa Conjecture. In this lecture, we cover the proof of [2]. However it is worth mentioning this more recent and stronger improvement by Lovett [7]:

**Theorem 1** *For any Boolean function  $f$ ,  $CC(f) \leq O(\sqrt{\text{rank}(M_f)} \cdot \log \text{rank}(M_f))$ .*

Although the gap between the upper and lower bound is still exponential, Lovett's upper bound is unconditional and much stronger. He also uses more traditional combinatorial methods, namely the discrepancy of low rank matrices. Using Fourier Analysis, Tsang et al. gave a similar bound for Boolean functions of the form  $f(x, y) = F(x \oplus y)$  [10]. Gavinsky and Lovett also showed [3] the following relationship between deterministic and randomized protocol:

**Theorem 2** *If  $f$  has a randomized protocol of communication cost  $c$  and  $M_f$  of rank  $r$ , then  $f$  has a deterministic protocol of cost  $O(c^2 \log^2 r)$ .*

We present the proof of Ben Sasson, Lovett and Zewi theorem, which states:

**Theorem 3** Assuming the Polynomial Freiman Rusza conjecture over  $\mathbb{F}_2^n$ , for any Boolean function  $f$ :

$$CC(f) \leq O\left(\frac{\text{rank}(M_f)}{\log \text{rank}(M_f)}\right)$$

We will present the proof in a bottom up manner, that is we prove the Communication Complexity results and introduce Additive Combinatorics tools as needed. We start by proving this powerful result from [8], by Nisan and Wigderson, which shows that the existence of large monochromatic rectangles is enough to get efficient deterministic protocols.

**Theorem 4** Let  $f$  be a Boolean function, and suppose  $M_f$  has rank  $r$  and a monochromatic submatrix of size at least  $2^{-O(r/\log r)}|M_f|$ , then  $f$  can be computed using  $O(r/\log r)$  bits of communication.

**Proof** Pick  $R$  to be a monochromatic submatrix of  $M_f$  of size at least  $2^{-O(r/\log r)}|M_f|$ , and partition  $M_f$  as follows:

$$\begin{bmatrix} R & S \\ P & Q \end{bmatrix}$$

Now pick  $r_S = \text{rank}(S)$  rows whose restriction to  $S$  are linearly independent, and similarly for  $r_P = \text{rank}(P)$  and  $P$ . Notice that if  $R$  is mono-chromatically 0 then the rows of  $M_f$  picked from  $S$  and  $P$  are linearly independent, and if  $R$  is mono-chromatically 1, then the rows picked from  $S$  and  $P$  are linearly independent, unless  $P$  has a row of all 1's (i.e., a row whose restriction to  $P$  is the all 1 vector), then this reduces the number of linearly independent vectors by at most 1, and thus:  $r_S + r_P \leq r + 1$ . Suppose without loss of generality that  $r_S \leq r + 1$ . The protocol goes as follows:

- For the first move, the row player (say Alice) sends Bob a bit encoding whether her input is in the first  $|R|$  rows or not, and the protocol proceeds recursively with a protocol for the sub-matrices  $[R \ S]$  or  $[P \ Q]$ .
- If Alice's input  $x$  is in the first  $R$  rows, then the rank of the new matrix is  $r_R + r_S \leq r/2$ .
- Otherwise  $x$  is in  $[P \ Q]$  which might not have smaller rank but we know has size at most  $(1 - 2^{-O(r/\log r)})|M_f|$ .

Consider the tree corresponding to this protocol and let  $L(m, r)$  denote the number of leaves in the protocol starting with a matrix of size at most  $m$  and rank at most  $r$ . We get the following recurrence:

$$L(m, r) \leq L(m, \frac{r}{2}) + L(m((1 - 2^{-O(r/\log r)})|M_f|), r)$$

Unwinding the recurrence gives us

$$\begin{aligned} L(m, r) &\leq 2^{2cr/\log r + O(\log^2 r)} \\ &\leq 2^{O(r \log r)} \end{aligned}$$

And now it suffices to use this classical result in CC:

**Theorem 5** *If  $f$  can be computed by a protocol with  $k$  leaves, then it can be computed by a protocol with  $O(\log k)$  bits of communication.*

to conclude that  $f$  can be computed using  $O(r \log r)$  bits.

Therefore to prove Theorem 2, we just need to show that every  $M_f$  contains a monochromatic submatrix  $M'$  of size at least  $2^{-O(r/\log r)}|M_f|$ . Notice that this was implicitly used in the proof above, namely when the protocol recurses on  $[R \ S]$  or  $[P \ Q]$ , it already assumes these sub-matrices also have monochromatic sub-matrices of proper sizes. Assuming the *Polynomial Freiman Ruzsa conjecture (PFR)*, Ben Sasson, Lovett and Zewi showed that such sub-matrices exist. In particular they switch from  $\mathbb{R}$  to  $\mathbb{F}_2$  to exploit the simple structure of  $\mathbb{F}_2$  and prove the following theorem:

**Theorem 6** *Assuming the PFR conjecture over  $\mathbb{F}_2^n$ , every  $0,1$ -matrix  $M$ , with no identical rows or columns has a monochromatic submatrix of size at least  $2^{-O(\text{rank}(M)/\log \text{rank}(M))}|M|$ .*

To prove Theorem 6, we introduce the notion of **duality** and **approximate duality**:

**Definition** For any  $A, B \subseteq \mathbb{F}_2^n$ , The duality measure of  $A, B$  is:

$$D(A, B) = \left| \mathbb{E}_{a \in A, b \in B} [(-1)^{\langle a, b \rangle}] \right|$$

where the inner product  $\langle a, b \rangle$  is done in  $\mathbb{F}_2$ . Notice that this definition of duality can be formulated to capture the discrepancy of the inner product function on the rectangle  $A \times B$  up to normalization:

$$D(A, B) = \left| \Pr_{a \in A, b \in B} [\langle a, b \rangle = 1] - \Pr_{a, b \in B} [\langle a, b \rangle = 0] \right|$$

In particular, for any matrix  $M$  with rank decomposition  $A, B$  over  $\mathbb{F}_2$  and discrepancy  $\delta(M)$ ,  $\delta(M) = D(A, B)$ . We say that  $A, B$  are **dual** if  $D(A, B) = 1$ . Notice that if  $M_f$  is a  $0, 1$  matrix with rank  $r = \text{rank}_{\mathbb{F}_2}(M_f)$ , and  $A^T B$  is the rank factorization of  $M_f$ , then  $D(A, B) = 1$  implies  $M_f$  is monochromatic.

The proof of Theorem 6 follows from the following lemma:

**Lemma 7 (Main Technical Lemma)** *Suppose  $A, B \subseteq \mathbb{F}_2^n$  satisfy  $D(A, B) \geq 2^{-\sqrt{n}}$ . Then assuming the PFR Conjecture, there exists subsets  $A' \subseteq A, B' \subseteq B$  such that  $D(A', B') = 1$  and  $|A'| \geq 2^{-cn/\log n}|A|, |B'| \geq 2^{-cn/\log n}|B|$  for some absolute constant  $c$ .*

and in particular, it follows from Lemma 8, a consequence of the Main Technical Lemma:

**Lemma 8** *Let  $M$  be a  $0, 1$ -matrix of rank at most  $r$  over  $\mathbb{F}_2$  and of discrepancy at least  $2^{-\sqrt{r}}$ . Assuming the PFR conjecture, there exists a monochromatic submatrix  $M'$  of  $M$  of size at least  $2^{-cr/\log r}|M|$  for some absolute constant  $c$ .*

**Proof** Let  $s$  denote the number of rows in  $M$  and  $t$  the number of columns in  $M$ . We know that  $\text{rank}(M)$  over a field  $\mathbb{F}$  is  $r$  iff  $M$  can be written as the sum of  $r$  rank one matrices over  $\mathbb{F}$ . Since  $\text{rank}_{\mathbb{F}_2}(M) \leq r$ , then there must exist subsets  $A, B \subseteq \mathbb{F}_2^r$   $A = \{a_1, a_2, \dots, a_s\}$  and  $B = \{b_1, b_2, \dots, b_t\}$  such that  $M_{i,j} = \langle a_i, b_j \rangle$  for all  $i \in [s], j \in [t]$ .

The main technical lemma implies the existence of  $A' \subseteq A, B' \subseteq B$  such that  $|A'| \geq 2^{-cr/\log r}|A|$

and  $|B'| \geq 2^{-cr/\log r}|B|$  and  $D(A', B') = 1$ .

Let  $M'$  be the submatrix of  $M$  whose rows and columns correspond to the indices in  $A'$  and  $B'$ , then:

$$D(A', B') = 1 \implies M_{i,j} = \langle a_i, b_j \rangle_2 \\ = \text{constant } \forall i, j$$

Therefore  $M'$  is monochromatic and satisfies

$$|M'| = |A'| |B'| \\ \geq 2^{-2cr/\log r} |A| |B| \\ = 2^{-2cr/\log r} |M|$$

In order to prove Theorem 6, we use Lemma 8 and the following result of Nissan and Wigderson [8]

**Theorem 9** *Every 0,1,matrix  $M$ , with  $r = \text{rank}(M)$ , has submatrix  $M'$  of size at least  $|M'| \geq r^{-3/2}|M|$  and  $\delta(M') \geq r^{-3/2}$ .*

**Proof** [of Theorem 6] Let  $r = \text{rank}(M)$ . Theorem 9 guarantees the existence of a submatrix  $M'$  of  $M$  such that  $|M'| \geq r^{-3/2}|M|$  and  $\delta(M') \geq r^{-3/2}$ . And Lemma 8 guarantees the existence of a monochromatic submatrix  $M''$  of  $M'$  of size at least  $|M''| \geq 2^{-cr/\log r}|M'|$  for some absolute constant  $c$ . So we have:

$$|M''| \geq 2^{-cr/\log r}|M'| \\ \geq 2^{-cr/\log r} r^{-3/2}|M| \\ = 2^{O(r/\log r)}|M|$$

Notice that all the inequalities hold because  $\text{rank}_{\mathbb{F}_2}(M') \leq \text{rank}(M') \leq \text{rank}(M) = r$ .

This concludes the proof of Theorem 6, which in turns concludes the proof of the main result. For the sake of completeness, we give a sketch of the Main Technical Lemma, this is where the heavy tools of additive combinatorics come into play. We first list the tools we need, namely the Polynomial Freiman-Ruzsa Conjecture, the Balog-Szemerédi-Gowers Theorem [1, 4], and the Approximate-Duality Lemma [11]

**Conjecture 1 (The Polynomial Freiman-Ruzsa Conjecture)** *There exists an absolute constant  $r$ , such that if  $A \subseteq \mathbb{F}_2^n$  has  $|A + A| \leq K|A|$ , then there exists a subset  $A' \subseteq A$  of size at least  $K^{-r}|A|$  such that  $|\text{span}(A')| \leq |A|$ .*

**Theorem 10 (The Balog-Szemerédi-Gowers Theorem)** *There exist fixed polynomials  $f(x, y), g(x, y)$  such that the following holds for every subset  $A$  of an Abelian additive group. If  $A$  satisfies  $\Pr_{a,a' \in A}[a + 1' \in S] \geq 1/K$  for  $|S| \leq C|A|$ , then one can find a subset  $A' \subseteq A$  such that  $|A'| \geq |A|/f(K, C)$ , and  $|A' + A'| \leq g(K, C)|A|$ .*

**Definition** : Given a set  $B \subseteq \mathbb{F}_2^n$  and  $\alpha \in [0, 1]$ , let the  $\alpha$ -spectrum of  $B$  be the set :

$$\text{Spec}_\alpha(B) = \{x \in \mathbb{F}_2^n \mid |\mathbb{E}_{b \in B}[(-1)^{\langle x, b \rangle_2}]| \geq \alpha\}$$

**Lemma 11 (The Approximate-Duality for sets with small span)** . If  $D(A, B) \geq \alpha$ , then there exists subsets  $A' \subseteq A, B' \subseteq B$  where  $|A'| \geq \frac{\alpha}{4}|A|$ ,  $|B'| \geq \frac{\alpha^2}{4} \frac{|A|}{|\text{span}(A)|} |B|$ , such that  $D(A', B') = 1$ . If  $A \subseteq \text{Spec}_\alpha(B)$  then we have  $|A'| \geq |A|/2$  and  $|B'| \geq \alpha^2 \frac{|A|}{|\text{span}(A)|} |B|$  in the statement above.

**Sketch of the Main Technical Lemma:** The main idea is given the two sets  $A$  and  $B$ , we keep generating new subsets  $A' \subseteq A, B' \subseteq B$  until we find a pair of subsets that have relatively large size and satisfy  $D(A', B') = 1$ .

By definition,  $A \subseteq \text{Spec}_\alpha(B) \implies D(A, B) \geq \alpha$ . In the other direction,  $D(A, B) \geq \alpha \implies \exists A' \subseteq A, |A'| \geq \frac{\alpha}{2}$  using Markov's inequality and  $A' \subseteq \text{Spec}_{\alpha/2}(B)$ . To prove the main lemma, we start with  $A_1 = A'$  and  $\alpha_1 = \alpha/2$  and construct a sequence of sets as follows:

$$\begin{aligned} A_2 &\subseteq A_1 + A_1 \\ A_3 &\subseteq A_2 + A_2 \\ &\dots \end{aligned}$$

Where each  $A_i$  is in the  $\text{Spec}_{\alpha_i}(B)$  and  $\alpha_i = \alpha_{i-1}^2$ .

Each  $A_i$  has size at most  $2^n$ , and since the  $A_i$  sequence is infinite but the  $A_i$ 's are subsets of  $\mathbb{F}_2^n$ , there must exist an index  $i$  such that  $i \leq n \log K$ ,  $K > 1$  for which  $|A_{i+1}| \leq K|A_i|$ . Pick the smallest index  $t$  satisfying this, and use the PFR conjecture and Theorem 10 to show that

$$|A_{t+1}| \leq K|A_t| \implies \exists A_t'' \subseteq A_t \text{ that has small span over } \mathbb{F}_2.$$

By construction  $A_t''$  satisfies  $D(A_t'', B) \geq \alpha_t$  since  $A_t'' \subseteq \text{Spec}_{\alpha_t}(B)$  and  $A_t''$  is a relatively large fraction of its span. Using the Approximate Duality Lemma (Lemma 11), we conclude that  $A_t''$  and  $B$  contain relatively large subsets  $A_t', B_t'$  such that  $D(A_t', B_t') = 1$ , i.e.  $A_t''$  and  $B$  contain **dual** large subsets  $A_t', B_t'$ . Again by construction  $A_t' \subseteq A_{t-1} + A_{t-1}$ , then  $A_{t-1}$  also contains a large subset  $A_{t-1}'$  dual to a large subset  $B_{t-1}' \subseteq B_t'$ ,  $D(A_{t-1}', B_{t-1}') = 1$ . We keep finding these dual pairs for values  $t-2, t-3, \dots, 1$  upon which we have found a dual pair of subsets of  $A$  and  $B$  with relatively large size.

**Conclusion:** As already stated, the result by Lovett is much stronger and tighter. In [9], Rothvoss presented a different proof to Lovett's upper bound. However these results still leave an exponential gap between an upper and lower bound, thus leaving much work to be done. An interesting direction is to see if the combination of these approaches (additive combinatorics, Fourier analysis and discrepancy of low-rank matrices) can help improve the gap.

## References

- [1] A. BALOG AND E. SZEMERÉDI, *A statistical theorem of set addition*, *Combinatorica*, 14 (1994), pp. 263–268.
- [2] E. BEN-SASSON, S. LOVETT, AND N. ZEVI, *An additive combinatorics approach to the log-rank conjecture in communication complexity*, arXiv preprint arXiv:1111.5884, (2011).
- [3] D. GAVINSKY AND S. LOVETT, *En route to the log-rank conjecture: New reductions and equivalent formulations.*, in *Electronic Colloquium on Computational Complexity (ECCC)*, vol. 20, 2013, pp. 6–15.

- [4] W. T. GOWERS, *A new proof of szemerédi's theorem for arithmetic progressions of length four*, Geometric and Functional Analysis, 8 (1998), pp. 529–551.
- [5] A. KOTLOV, *Rank and chromatic number of a graph*, Journal of Graph Theory, 26 (1997), pp. 1–8.
- [6] L. LOVÁSZ AND M. SAKS, *Lattices, mobius functions and communications complexity*, in 2013 IEEE 54th Annual Symposium on Foundations of Computer Science, IEEE, 1988, pp. 81–90.
- [7] S. LOVETT, *Communication is bounded by root of rank*, arXiv preprint arXiv:1306.1877, (2013).
- [8] N. NISAN AND A. WIGDERSON, *On rank vs. communication complexity*, Combinatorica, 15 (1995), pp. 557–565.
- [9] T. ROTHVOSS, *A direct proof for lovett's bound on the communication complexity of low rank matrices*, arXiv preprint arXiv:1409.6366, (2014).
- [10] H. Y. TSANG, C. H. WONG, N. XIE, AND S. ZHANG, *Fourier sparsity, spectral norm, and the log-rank conjecture*, in Foundations of Computer Science (FOCS), 2013 IEEE 54th Annual Symposium on, IEEE, 2013, pp. 658–667.
- [11] N. ZEVI AND E. BEN-SASSON, *From affine to two-source extractors via approximate duality*, in Proceedings of the forty-third annual ACM symposium on Theory of computing, ACM, 2011, pp. 177–186.