Dimension-free Bounds and Structural Results in Communication Complexity

Lianna Hambardzumyan

School of Computer Science

McGill University, Montreal

August, 2021

A thesis submitted to McGill University in partial fulfillment of the requirements of the degree of Doctor of Philosophy

Abstract

The goal of this thesis is to continue to build the bridge between communication complexity and analysis. More specifically, the purpose is to initiate a systematic study of *dimension-free* relations between basic *communication complexity* and *query complexity* measures and various *matrix norms*. In other words, our goal is to establish *qualitative equivalences* between complexity measures, namely to bound a measure solely as a function of another measure. This is in contrast to the more common framework in communication complexity where quantitative equivalences are the main focus of study and poly-logarithmic dependencies on the number of input bits are tolerated.

Dimension-free bounds are closely related to structural results, where one seeks to describe the structure of Boolean matrices and functions that have low complexity. We restate and propose several conjectures in this nature such as: *Does every matrix with small randomized communication complexity contain a large all-zero or all-one submatrix* [CLV19]? *Does every Boolean function with small approximate Fourier algebra norm have large affine subspace on which the function is constant?*

We consider such questions for several communication and query complexity measures as well as various matrix and operator norms. In several cases, we achieve satisfying answers, while for some cases we show that such bounds do not exist.

We establish that, in addition to applications in complexity theory, these problems arise naturally in operator theory and Harmonic analysis. We show that these problems are central to characterization of the idempotents of the algebra of Schur multipliers, and could lead to new extensions of Cohen's celebrated idempotent theorem regarding the Fourier algebra.

Abrégé

L'objectif de cette thèse est de renforcer le lien entre les domaines de la complexité de la communication et l'analyse. Plus précisément, son but est d'initier une étude systématique des relations entre la *complexité de la communication* basique et la *complexité des requêtes* et de diverses *normes de matrice* indépendamment des dimensions. En d'autres mots, notre objectif est d'établir des équivalences qualitatives entre les mesures de la complexité, à savoir pour lier une mesure uniquement en fonction d'une autre mesure. Cela diffère du cadre habituel de la complexité de la communication, où l'emphase est plutôt mise sur l'étude des équivalences quantitatives et où les dépendances polylogarithmiques sur le nombre de bits dans les données sont tolérées.

Les limites indépendantes des dimensions sont fortement liées aux résultats structuraux, où l'un cherche à décrire la structure des matrices booléennes et des fonctions de basse complexité. Ainsi, nous reformulons et proposons plusieurs hypothèses : *Est-ce que toutes les matrices dont la complexité de communication aléatoire est basse ont des sous-matrices larges de 0 ou de 1 [CLV19]? Est-ce que toutes les fonctions booléennes, dont les normes d'algèbre de Fourier approximatives sont petites, ont des sous-espaces affines larges sur lesquels la fonction est constante?*

Nous considérons de telles questions pour les mesures de la complexité de communication et des requêtes ainsi que pour diverses normes de matrices et d'opérateurs. Dans plusieurs cas, nous avons obtenu des réponses satisfaisantes. Cependant, dans certains cas, nous montrons que de telles limites n'existent pas.

Nous établissons qu'en plus de leur application dans la théorie de la complexité, ces problèmes apparaissent naturellement en théorie des opérateurs ainsi qu'en analyse harmonique. Nous montrons que ces problèmes sont importants pour la caractérisation des idempotentes de l'algèbre des multiplicateurs de Schur et qu'ils pourraient mener à de nouvelles extensions du théorème des idempotentes célébré de Cohen sur les algèbres de Fourier.

Acknowledgements

I am indebted to my supervisor, Hamed Hatami, without whose constant support I would never have been able to go through graduate studies, let alone write this thesis. Thank you for introducing me to Communication Complexity, Fourier analysis, and so much more – I'm yet to discover the limits of your knowledge in math. Thanks for letting me work with you despite my never-ending stream of questions and a special thanks for not leaving a single question unanswered. Thanks for teaching me how to do research at every step of the making – from "which are the nice problems to choose" and "how to work while taking a long walk to the climbing gym", to "how to write a paper which is rigorous but not painful to read." Thanks for constantly pushing me to do a lot more than I ever thought myself capable of doing. And, of course, I cannot thank you enough for pushing me into climbing and teaching me the basics while resisting my hesitance – both this work and I have benefited from the steady supply of endorphins and problem-solving techniques adopted from climbing. Lastly, thanks for also being a caring friend; all that you have done for me, I can only hope to pay it forward.

I am forever thankful to Prakash Panangaden for being my co-supervisor during the first years of my studies. It goes without saying that I wouldn't have ended up at McGill without you. Thanks for believing in me (I still can't believe my luck), for bringing me to McGill and funding me in the beginning, for your contagious enthusiasm and positivity, for teaching me Information theory, and for telling me "go do the math that's fun for you."

I am grateful to Pooya Hatami at Ohio State University for bringing his passion and knowledge to this project, for pushing me to work harder, and for his patience with me.

I am indebted to Luc Devroye for teaching me a fair bit of probability theory, for being an awesome spirit across the hall, and for fighting for my funding. Because Luc is a black belt level fighter, my studies have partially been supported by the "Women in Science" fellowship at McGill – I am grateful to the fellowship, for all the opportunities it made possible for me.

In particular, due to the fellowship, I had the privilege of spending a semester at Simons Institute. I am thankful to Hamed and the institute for hosting me. The vibrant community there opened the world of complexity theory for me (then plunged me deep into it for a semester!), and planted the seeds for this work. Thanks to the amazing people there that shared their knowledge, particularly to Robert Robere for teaching me a great deal of complexity theory and cool math; to Yuval Filmus for educating me on TCS in general; to Avishay Tal and Shachar Lovett for sharing their insight on pseudorandomness.

Thanks are due to my teachers who set me on this path; to Vahan Mkrtchyan for introducing me to Graph theory during my Bachelor's, and for blindly believing in me and encouraging me to do research; to my high school math teacher Eduard Mkrtchyan for teaching me how to think and for reminding me that you are a kettle (i.e. dumb) as long as you haven't asked your question; to my mom for never explaining any math notation or solution to me, but rather guiding me to understanding on my own, thus letting me experience the joy of discovery – little did she know I'd get hooked.

To Liana Yepremyan, whose one suggestion ("Why don't you come to McGill?") started this great journey. Thanks for holding my hand during the hard moments of this path, for treating my problems as your own, and for showing me that the line between what's possible and what's impossible is thin and breakable.

I want to also thank a few people who supported me during my studies. For their friendship at McGill, for enlightening chats, and for advice: Mash, Xing Shi Cai, Yaqiao, Lena, Richard, Jan, Vishnu, Stefan, Ndiamé. Thanks to Mash and Cai for their moral support from the first day to the last, and for always being eager to come up with answers to any of my questions – be it math or philosophy. To all my friends in Montreal and elsewhere, especially to Pierre-William and Lili for being a good company in all of these years, to Astrid for proofreading parts of this thesis, to Mika for his help along the way, to Arevik for being there for (and with) me in the worst of times and the best of times.

Finally, I am thankful to my family; to my grandma for being a loving source of strength and wisdom; to my brother for being my rock back home, and to my mom for making me laugh all the time and for imprinting in me that math is fun and should always be fun.

Lastly, I am thankful to the reviewers of this thesis, Arkadev Chattopadhyay and Luc Devroye, for their time and valuable comments that improved the thesis.

Dedication

To my mom, my grandma and my brother

Contribution

Work included The novel parts of this thesis are Chapters 4, 5, 6 and 7. These are based on the following joint work. Section 4.6 is not included in any manuscript.

- L. Hambardzumyan, Hamed Hatami and Pooya Hatami. "Dimension-free Bounds and Structural Results in Communication Complexity" (accepted to *Israel Journal of Mathematics*).

Work not included During my PhD studies I have also co-authored several papers that are not included in this thesis as they are outside of complexity theory and do not fit the theme of the thesis.

- Yuval Filmus, L. Hambardzumyan, Hamed Hatami, Pooya Hatami, David Zuckerman. "Biasing Boolean Functions and Collective Coin-Flipping Protocols over Arbitrary Product Distributions". *46th International Colloquium on Automata, Languages, and Programming (ICALP 2019)*, volume 132 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 58:1-58:13, Dagstuhl, Germany, 2019. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik.

- L. Hambardzumyan and Yaqiao Li. "Chang's lemma via Pinsker's inequality". *Discrete Math.*, 343(1):111496, 3, 2020.

- L. Hambardzumyan, Hamed Hatami, and Yingjie Qian. "Lower bounds for graph bootstrap percolation via properties of polynomials". *J. Combin. Theory Ser. A*, 174:105253, 12, 2020.

Table of Contents

Chapter 1

Introduction

A matrix is called *Boolean* if its entries are either 0 or 1, and similarly, a function is called *Boolean* if it takes only 0 and 1 values. Our goal in this thesis is to study whether dimension-free relations exist between basic communication and query complexity measures and various matrix norms for Boolean matrices and functions.

The field of communication complexity, formally defined in 1979 in a paper by Yao [Yao77], studies the communication costs of computing Boolean functions whose input is split between two or more parties. In the two-party model, two players, Alice and Bob, want to collaboratively compute a Boolean function (or a matrix) $f : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ [1]. Alice and Bob are given inputs $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, respectively. Neither of the players knows the other's input, however, the function f is known to both players. They have access to unlimited computational power, and wish to compute $f(x, y)$ by transmitting the *minimum* number of bits. This transmission is carried out according to a communication algorithm π – referred to as *protocol* throughout the text – which is fixed by Alice and Bob beforehand, and depends only on the task f. The number of bits transmitted according to a protocol on the worst input is called the *cost* of the protocol.

The *deterministic communication complexity* of f, denoted by $\mathrm{D}(f)$, is the number of bits Alice and Bob have to exchange according to the best protocol on the worst case choice

[1] Throughout the text we refer $f : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ as a matrix and a function interchangeably.

of input pair (x, y), i.e.

$$\mathrm{D}(f) = \min_{\pi} \max_{(x,y)\in\mathcal{X}\times\mathcal{Y}} \{\text{number of bits exchanged by } \pi \text{ to compute } f(x, y)\}.$$

Obviously, one of the parties, say Alice, can send her entire input, bit by bit, to Bob, he then can evaluate f on their inputs, and send the output back to Alice [2].

Thus, $1 \leq D(f) \leq \min\{\log(|\mathcal{X}|), \log(|\mathcal{Y}|)\} + 1$ for every f. While for some functions this trivial algorithm is provably optimal, the goal is to find better bounds for communication complexity, or for certain functions, exactly determine it.

Allowing Alice and Bob to have access to a source of randomness can make communication protocols more powerful. Given a source of randomness, Alice's and Bob's next messages not only depend on the previous messages but also on a coin flip. Hence, the output of the function will also depend on the sequence of coin flips. Here, we will allow the protocols to output a wrong value with a small probability. We say that a protocol uses the *public coin* model if Alice and Bob receive the same random string r. Then they execute a deterministic protocol π_r, where their messages can depend on the string r. In other words, a randomized communication protocol is a distribution over deterministic protocols. A randomized protocol computes a function f with error at most ϵ if $\Pr_r[\pi_r(x, y) = f(x, y)] > 1 - \epsilon$ for every input (x, y). The cost of a public coin protocol is the maximum cost of any of the deterministic protocols π_r. The *public coin randomized communication complexity* of f, denoted by $\mathrm{R}_\epsilon(f)$, is the *minimum* cost of a public coin protocol which computes f with error at most ϵ.

Developed by complexity theorists, communication complexity has been naturally influenced by the more classical areas of complexity theory such as computational complexity where the main challenges lie in separation of complexity classes. Communication complexity classes are defined in [BFS86] as the set of problems that can be solved using protocols with communication costs $\log^c(n)$ in the corresponding model, where n is the number of input bits. As a result, a major part of the literature of communication complexity is focused

[2] We follow the convention that the last communicated bit must be the output bit, otherwise $D(f) \geq 1$ is not true when f is a constant function.

on finding explicit instances (e.g. set-disjointness [She14], Hadamard matrix [For02], gap Hamming distance [CR12]) that require communication cost $\log^c(n)$ in one model (e.g. non-deterministic), whereas they require a much higher communication cost in a different model (e.g. randomized), ideally $\Omega(n)$. However, a $O(\log(n))$ versus $\Omega(n)$ separation unfortunately does not overrule the existence of dimension-free relations, as for instance, it is possible that one parameter is upper-bounded by an exponential function in the other parameter.

A relation between two measures is called a *dimension-free relation* or *bound* if it provides a bound on one of the measures solely as a function of another one. Dimension-free bounds are often closely related to structural results. For instance, it is well-known that if the deterministic communication complexity of a Boolean function is bounded by a constant c, then its corresponding matrix is highly structured. Namely, it can be partitioned into 2^c all-zero or all-one submatrices. In other words, its *partition number* is upper-bounded by a constant. Similarly, its rank is also upper-bounded by 2^c.

The simple example of the identity matrix, often called the *equality function* in the context of communication complexity, shows that having small *randomized* communication complexity does not imply a small partition number or a small rank, as the $n \times n$-sized identity matrix has rank n, partition number $\Omega(n)$ and randomized communication complexity $O(1)$. While this and a handful of other known examples show that the rank of a matrix with bounded randomized communication complexity can be arbitrarily high, they do not overrule the possibility that such matrices might be structured in a different way, or at least contain highly structured parts. Investigating such structures is another focus of this thesis.

All the known examples of matrices with small randomized communication complexity contain a large all-zero or all-one submatrix. The following conjecture in [CLV19], speculates that this structure holds in general.

Conjecture I. *If the randomized communication complexity of an $n \times n$ Boolean matrix M is bounded by c, then it contains an all-zero or all-one $\delta_c n \times \delta_c n$ submatrix, where $\delta_c > 0$ is a constant that only depends on c.*

In fact [CLV19] conjectures that one can take $\delta_c = 2^{-O(c)}$ in the above statement. Another motivation for this conjecture stems from the open question of separating communication complexity classes $\mathbf{BPP}^{\mathrm{CC}}$ and $\mathbf{P}^{\mathbf{NP}^{\mathrm{CC}}}$ posed by [GPW18b] (see Section 2.6).

One way to establish Conjecture I would be to show that every Boolean matrix with small parameter τ contains a large constant submatrix, where τ is a matrix parameter lower-bounding randomized communication complexity. It is well-known that the normalized approximate trace norm of a matrix is such a parameter. The *approximate trace norm* $\|M\|_{\mathrm{tr},\varepsilon}$ for some $\varepsilon > 0$ is defined as the smallest $\|M'\|_{\mathrm{tr}}$ for a real matrix M' such that $|M(i,j) - M'(i,j)| \leq \varepsilon$ for every i, j. It provides a lower bound of $\Omega\left(\log \frac{\|M\|_{\mathrm{tr},\varepsilon}}{n}\right)$ for the randomized communication complexity (see Lemma 2.15). Hence, this motivates us to ask the following tantalizing question about the trace norm itself.

Conjecture II. *If an $n \times n$ Boolean matrix M satisfies $\frac{\|M\|_{\mathrm{tr}}}{n} \leq c$, then it contains an all-zero or all-one $\delta_c n \times \delta_c n$ submatrix, where $\delta_c > 0$ is a constant that only depends on c.*

This conjecture is interesting also from the point of view of graph theory. The trace norm of the adjacency matrix of a graph is considered an important graph parameter, and is often called *graph energy* [LSG12] in that context. Furthermore, there is an extensive body of research that investigates graph theoretic [Chu14] or spectral conditions [GN08, BN07, Nik06, LLT07, Nik09] that guarantee the existence of large complete bipartite subgraphs in a graph or its complement. Conjecture II, if true, provides a very natural condition based on graph energy.

The motivation behind the subject of this thesis goes beyond communication complexity and combinatorics. Several of the problems considered in this thesis are basic questions about Boolean matrices, and unsurprisingly, they also arise naturally in other areas of mathematics such as *operator theory*, and *Harmonic analysis.*

Connection to Operator theory. Let $\mathcal{X}$ and $\mathcal{Y}$ be fixed countable sets, finite or infinite, and consider the set of $\mathcal{X} \times \mathcal{Y}$ Boolean matrices $M : \mathcal{X} \times \mathcal{Y} \to \{0, 1\}$. We shall think of rank-one Boolean matrices as the most structured of those. Every such matrix is of the form $\mathbf{1}_{\mathcal{X}_0} \otimes \mathbf{1}_{\mathcal{Y}_0}^{\mathrm{T}}$ for some $\mathcal{X}_0 \subseteq \mathcal{X}$ and $\mathcal{Y}_0 \subseteq \mathcal{Y}$. These matrices, which correspond to *combinatorial* *rectangles* $\mathcal{X}_0 \times \mathcal{Y}_0 \subseteq \mathcal{X} \times \mathcal{Y}$, are the building blocks of communication complexity. We denote by

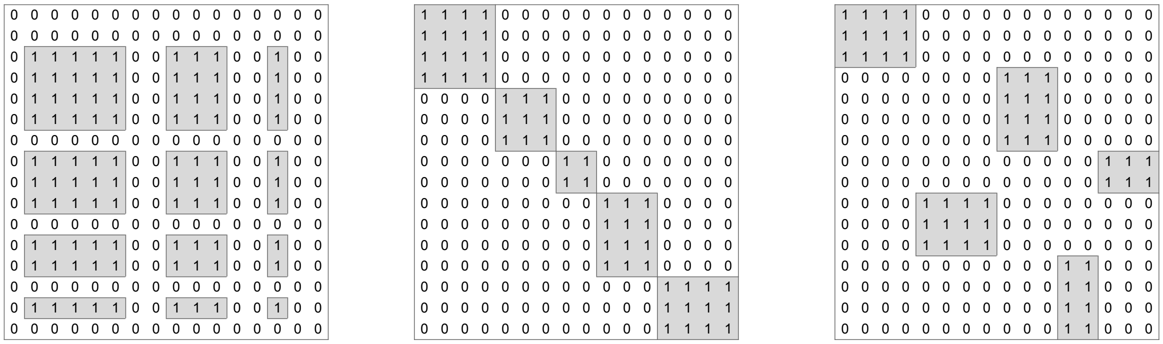
$$\mathscr{Rect} = \{M : \mathcal{X} \times \mathcal{Y} \to \{0,1\} \mid \mathrm{rk}(M) = 1\},$$

the set of all rank-one Boolean matrices.

The next important class of structured Boolean matrices for the purposes of this thesis is defined as follows. We call a matrix $M : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ *blocky* if there exist, possibly infinitely many, disjoint sets $\mathcal{X}_i \subseteq \mathcal{X}$ and disjoint sets $\mathcal{Y}_i \subseteq \mathcal{Y}$ such that the support of M is

$$\bigcup_i \mathcal{X}_i \times \mathcal{Y}_i.$$

A simple example of a blocky matrix is the *identity matrix*. We denote by $\mathscr{Blocky}$ the set of all blocky matrices. Figure 1.1 demonstrates examples of a combinatorial rectangle, and blocky matrices.



$$\begin{matrix}
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&1&1&1&1&0&0&1&1&1&0&0&1&0&0\\
0&1&1&1&1&1&0&0&1&1&1&0&0&1&0&0\\
0&1&1&1&1&1&0&0&1&1&1&0&0&1&0&0\\
0&1&1&1&1&1&0&0&1&1&1&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&1&1&1&1&0&0&1&1&1&0&0&1&0&0\\
0&1&1&1&1&1&0&0&1&1&1&0&0&1&0&0\\
0&1&1&1&1&1&0&0&1&1&1&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&1&1&1&1&0&0&1&1&1&0&0&1&0&0\\
0&1&1&1&1&1&0&0&1&1&1&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&1&1&1&1&0&0&1&1&1&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{matrix}
\qquad
\begin{matrix}
1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&1&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&1&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&1&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&1&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&1&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&1&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&1&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1
\end{matrix}
\qquad
\begin{matrix}
1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&1&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&1&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&1&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&1&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1\\
0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0\\
0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0\\
0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0
\end{matrix}$$

Figure 1.1: A combinatorial rectangle on the left, and a blocky matrix on the middle and on the right.

Blocky matrices appear naturally in different contexts, including those related to the topic of this thesis, and have been given different names. In graph theory, blocky matrices correspond to equivalence relations on the vertex set of a graph, and thus they have been called *equivalence graphs* [Duc79, Fra82, Alo86, BK95]. In complexity theory, blocky matrices have found applications in proving bounds against circuits and branching programs [PR94, Juk06].

A blocky matrix is essentially a blow-up of the identity matrix, obtained by duplicating rows and columns, and then permuting them. Hence, similar to the identity matrix, the randomized communication complexity of every finite blocky matrix is bounded by a fixed constant.

Blocky matrices also arise in the context of Schur multipliers. Recall that the *Schur product* (also called the Hadamard product) of two $|\mathcal{X}| \times |\mathcal{Y}|$ matrices M_1 and M_2, denoted by $M_1 \circ M_2$, is their entry-wise product. Let $B(\mathcal{X}, \mathcal{Y})$ denote the space of bounded linear operators $A : \ell_2(\mathcal{X}) \to \ell_2(\mathcal{Y})$ endowed with the operator norm. A $|\mathcal{X}| \times |\mathcal{Y}|$ matrix M is called a *Schur multiplier* if for every $A \in B(\mathcal{X}, \mathcal{Y})$, we have $M \circ A \in B(\mathcal{X}, \mathcal{Y})$. Every Schur multiplier M defines a map $B(\mathcal{X}, \mathcal{Y}) \to B(\mathcal{X}, \mathcal{Y})$ via $A \mapsto M \circ A$, which assigns an operator norm to it:

$$\|M\|_m \coloneqq \|M\|_{B(\mathcal{X},\mathcal{Y}) \to B(\mathcal{X},\mathcal{Y})} = \sup\{\|M \circ A\|_{\ell_2(\mathcal{X}) \to \ell_2(\mathcal{Y})} : \|A\|_{\ell_2(\mathcal{X}) \to \ell_2(\mathcal{Y})} \leq 1\}.$$

Note that Schur multipliers form a *Banach algebra* via Schur product:

$$\|M_1 \circ M_2\|_m \leq \|M_1\|_m \|M_2\|_m.$$

An element a of an algebra is said to be *idempotent* if $a^2 = a$. The following question arises naturally.

What are the *idempotents* of the algebra of Schur multipliers?

Every idempotent of this algebra must satisfy $M = M \circ M$, and thus is a Boolean matrix. However, not every (infinite) Boolean matrix is a bounded Schur multiplier, as it is possible to have $\|M\|_m = \infty$ for a Boolean matrix M [Liv95]. It is shown by Livshits in [Liv95] that blocky matrices are exactly the set of all *contractive* idempotents, meaning, an idempotent Schur multiplier satisfies $\|M\|_m \leq 1$ if and only if it is a blocky matrix. Livshits's characterization of idempotent Schur multipliers has been extended to other related settings [BH04, Neu06, KP05, Lev14, MP16]. An important question in this area (see e.g. [ELT16]) is the following.

> Are the idempotent Schur multipliers exactly those Boolean matrices that can be written as a linear combination of *finitely* many contractive idempotents (or equivalently blocky matrices)?

A simple compactness argument, as outlined in Theorem 4.12, shows that this problem is equivalent to the following basic question about Boolean matrices.

Conjecture III. *For every $c > 0$, there exists $k_c \in \mathbb{N}$ such that the following holds. If a finite Boolean matrix M is a linear combination of rank-one Boolean matrices with coefficients λ_i satisfying $\sum_i |\lambda_i| \leq c$, then M is a ± 1-linear combination of at most k_c blocky matrices.*

On the other hand, it is not difficult to see that if M is a ± 1-linear combination of at most k_c blocky matrices, then M can be written as a linear combination of rank-one Boolean matrices with coefficients whose absolute values sum to at most $O(k_c)$.

By Grothendieck's inequality (see Theorem 2.10), the assumption in Conjecture III can be equivalently replaced with the bound $\|M\|_{\gamma_2} = O(1)$, where

$$\|M\|_{\gamma_2} \coloneqq \min\{\|B\|_{2\to\infty}\|C\|_{1\to 2} \ : \ M = BC\}.$$

The connection to Schur multipliers is due to the fact, stated in Theorem 2.10, that γ_2 norm coincides with the norm of M as a Schur multiplier.

Connection to Harmonic analysis. Let G be a locally compact Abelian group with the dual group $\widehat{G}$. Let $\mathbf{M}(G)$ denote the *measure algebra* of G, that is to say the algebra of bounded, regular, complex-valued measures on G with the convolution operator as multiplication (denoted by $*$). Note that every idempotent μ of this algebra satisfies $\mu * \mu = \mu$, and this is equivalent to the statement that the Fourier transform $\widehat{\mu}$ satisfies $\widehat{\mu}^2 = \widehat{\mu}$, and thus is Boolean. Paul Cohen, in a celebrated article [Coh60], proved that μ is an idempotent if and only if $\widehat{\mu}$ can be expressed as a ± 1-linear combination of the indicator functions of a finite number of cosets of $\widehat{G}$. More recently, Green and Sanders [GS08], and Sanders [San20] have proven effective bounds on the required number of cosets as a function of $\|\mu\|$ when G is finite.

As we explain below, Cohen's idempotent theorem is closely related to Conjecture III. Consider a *finite* Abelian group G. In this case, since $G \cong \widehat{G}$, and $\mathbf{M}(G) = L^1(G)$, by switching the roles of G and $\widehat{G}$, one can state Cohen's idempotent theorem as follows.

Theorem 1.1 (Cohen's theorem)**.** *For every $c > 0$, there exists $k_c > 0$ such that the following holds: If $f : G \to \{0,1\}$ satisfies*

$$\|f\|_A := \sum_{\chi \in \widehat{G}} |\widehat{f}(\chi)| \leq c, \tag{1.1}$$

then

$$f = \sum_{i=1}^{k_c} \pm \mathbf{1}_{H_i + a_i}, \tag{1.2}$$

where each $H_i \leq G$ is a subgroup, and each $a_i \in G$.

The norm $\|\cdot\|_A$ is called the *Fourier algebra norm*, and for finite Abelian groups, it is equal to the sum of absolute values of Fourier coefficients of the function.

Note that $\|\mathbf{1}_{H_i+a_i}\|_A = 1$, and furthermore it is not difficult to prove that the indicator functions $\mathbf{1}_{H+a}$ of cosets are the only non-zero contractive idempotents of the Fourier algebra. This is called the Kawada-Itô theorem [KI40, Theorem 3] and dates back to 1940. In other words, if $f : G \to \{0,1\}$ satisfies $\|f\|_A = 1$, then $f = \mathbf{1}_{H+a}$ for some coset $H + a$. Hence, Cohen's idempotent theorem says that every idempotent of the Fourier algebra of G can be expressed as a linear combination of $\kappa(\|f\|_A)$ many *contractive* idempotents for some function $\kappa(\cdot)$. This is precisely what Conjecture III is trying to establish regarding the idempotents of the algebra of Schur multipliers. As we explain below, this connection is more than just a verbal analogy.

Let G be a finite Abelian group. Consider a Boolean $f : G \to \{0,1\}$ satisfying (1.1), and let the Boolean matrix $F : G \times G \to \{0,1\}$ be defined as $F(x,y) = f(x-y)$. It is well-known [LS09, Lemma 36] that

$$\|F\|_{\gamma_2} = \frac{\|F\|_{\mathrm{tr}}}{|G|} = \sum_{\chi \in \widehat{G}} |\widehat{f}(\chi)| = \|f\|_A. \tag{1.3}$$

Hence if $\|f\|_A \leq c$, then the assumption of Conjecture III holds for F, and if the conjecture is true, one should be able to express F as a linear combination of a bounded number (as a function of c) of blocky matrices. Indeed in this case, Conjecture III follows from Cohen's idempotent theorem, since a coset $\mathbf{1}_{H_i+a_i}$ in (1.2) corresponds to the blocky matrix supported on the entries in

$$\bigcup_{b \in G/H} (H_i + b) \times (H_i + b - a_i).$$

Thus Cohen's idempotent theorem implies that both Conjecture II and Conjecture III are true for matrices of the form $F(x, y) = f(x - y)$. In this regard, Conjecture III can be thought of as an extension, or more accurately, an analogue of Cohen's idempotent theorem for the algebra of Schur multipliers. Obviously due to lack of structure in a group, one cannot hope to find cosets—instead Conjecture III promises blocky matrices.

Finally, let us discuss the *approximate* version of Cohen's idempotent theorem, significant to us due to connections to randomized query and communication complexity. Let G be an Abelian group, and let $f : G \to \{0, 1\}$ be a Boolean function. Now, instead of assuming that $\|f\|_A$ is small, let us assume a weaker condition – f has an approximator with small algebra norm. More precisely, there exists a function $g : G \to \mathbb{R}$, not necessarily Boolean, such that $\|f - g\|_\infty \le \epsilon$ and $\|g\|_A \le c$. Such functions have been studied by Méla [M8́2] and Host, Méla, and Parreau [HMP86] under the name *ϵ-quasi-idempotent*. In [M8́2] Méla shows that in general, a structure similar to Cohen's idempotent theorem does not necessary hold for such functions. However, in the spirit of Conjecture I, we conjecture that for $G = \mathbb{Z}_2^n$, every *ϵ-quasi-idempotent* contains a highly structured part.

Conjecture IV. *Let $f, g : \mathbb{Z}_2^n \to \mathbb{R}$ be such that f is Boolean, $\|f - g\|_\infty \le \frac{1}{3}$, and $\|g\|_A \le c$. There exists a coset $V = H + a \subseteq \mathbb{Z}_2^n$ such that f is constant on V, and $\frac{|V|}{|\mathbb{Z}_2^n|} \ge \delta_c > 0$, where $\delta_c > 0$ is a constant that only depends on c.*

The constant $\frac{1}{3}$ in the statement is not important and can be replaced by any fixed constant $\epsilon \in (0, 1/2)$, as it is not difficult to see that all such statements will be equivalent.

Conjecture IV, if true, would imply Conjecture I for matrices of the form $F(x, y) = f(x - y)$ where $f : \mathbb{Z}_2^n \to \{0, 1\}$. Indeed, this follows from the fact that randomized communication complexity upper-bounds the approximate trace norm, and Proposition 4.13 (a generalization of Equation (1.3)) applied to the following symmetrization of the function $G(x,y)$ approximating $F(x,y)$

$$\tilde{G}(x,y) \coloneqq \mathbb{E}_z \left[G(z+x, z+y) \right].$$

Public-coin versus private-coin randomness: In the *private-coin* model, each party privately samples an independent random string. We caution the reader that in this thesis, randomized communication complexity always refers to the *public-coin model* – where randomness is shared between the players – unless the opposite is stated explicitly. We also reserve the notation $\mathrm{R}(M)$ to denote the public-coin randomized communication complexity of a Boolean matrix M. See Section 2.1.2 for formal definitions.

Qualitative versus quantitative, and dimension-free-ness: In this thesis we are interested in *dimension-free* results. In other words, we call two parameters *qualitatively equivalent* if each can be bounded as a function of solely the other one. Furthermore, since the main purpose of this thesis is establishing dimension-free dependencies, we will not be concerned with quantitative effectiveness of these bounds.

For example, the well-known relations

$$\log \mathrm{rk}(M) \leq \mathrm{D}(M) \leq \mathrm{rk}(M), \tag{1.4}$$

between rank and deterministic communication complexity, show that insofar as this thesis is concerned, they are qualitatively equivalent. In contrast, despite Newman's theorem [New91], which states that for $n \times n$ matrices,

$$\mathrm{R}(M) \leq \mathrm{R}^{\mathrm{private}}(M) \leq O(\mathrm{R}(M) + \log\log(n)), \tag{1.5}$$

due to the $\log\log(n)$ term (which is necessary), public and private randomized communication complexities are not qualitatively equivalent.

In fact, the private-coin model is not interesting from our standpoint: For every Boolean matrix M,

$$\Omega(\log \mathrm{D}(M)) = \mathrm{R}^{\mathrm{private}}(M) \leq \mathrm{D}(M),$$

and thus, as far as this thesis is concerned, the private-coin randomized communication complexity is qualitatively equivalent to the deterministic communication complexity [KN97, Lemma 3.8].

1.1 Our contributions

In this section, we summarize some of the results proven in this thesis.

- In Section 4.1 we prove that the deterministic communication complexity with access to an equality oracle is qualitatively equivalent to the smallest k such that the matrix can be written as a linear combination of k blocky matrices.

- In Section 4.2, we show that *zero-error* randomized communication complexity and rank are qualitatively equivalent. Consequently, combining this with a recent result of Gál and Syed [GS19] establishes qualitative equivalence between approximate rank, zero-error randomized communication complexity, deterministic communication complexity, and rank.

- In Section 4.3, we establish Conjecture I for one-sided error randomized communication complexity.

- In Section 4.4, in Theorem 4.12 we use a compactness argument to show that Conjecture III is equivalent to the statement that every idempotent of the algebra of Schur multipliers is a linear combination of finitely many contractive idempotents.

- In Section 4.5, we consider matrices that are constructed from functions on finite groups. Cohen's idempotent theorem has been generalized to hold for non-Abelian groups as well by Lefranc [Lef72], and effective bounds were given by Sanders [San11]. We use these results, in conjunction with a theorem of Davidson and Donsig [DD07] to verify Conjecture II and Conjecture III for matrices of the form $F(x, y) = f(y^{-1}x)$, where $f : G \to \{0, 1\}$ and G is any finite group.

- In Section 4.6, we prove a version of Conjecture IV for approximate Fourier rank instead of approximate Fourier algebra, which is a weakening of the conjecture.

- In Chapter 5, we consider XOR-lifts $F_{\oplus}(x,y) = f(x_1 \oplus y_1, \ldots, x_n \oplus y_n)$, where $f : \{0,1\}^n \to \{0,1\}$. Note that XOR-lift is a special case of $F(x,y) = f(y^{-1}x)$, where $G = \mathbb{Z}_2^n$, and thus, as we mentioned above, Conjecture II and Conjecture III are true for these matrices. We further discuss the analogue of Conjecture I for the $\oplus$-query model, i.e. for *parity decision trees*. In other words, we consider Conjecture IV in relation to randomized $\oplus$-query complexity. Furthermore, we show that the zero-error randomized $\oplus$-query complexity is qualitatively equivalent to both the deterministic $\oplus$-query complexity and the number of non-zero Fourier coefficients.

- In Chapter 6, we consider AND-lifts $F_{\wedge}(x,y) = f(x_1 \wedge y_1, \ldots, x_n \wedge y_n)$ for $f : \{0,1\}^n \to \{0,1\}$. We prove that the analogue of Conjecture IV is true in the $\wedge$-query model. Namely, in Theorem 6.3, we prove that if the randomized AND-decision tree of $f : \{0,1\}^n \to \{0,1\}$ is small, then there is a small set J of coordinates such that f is constant on $\{x : x_j = 0 \ \forall j \in J\}$.

  We remark that Conjecture I, Conjecture II and Conjecture III all remain unresolved for AND-lifts.

- In Chapter 7, we explain our failure in proving Conjecture I, Conjecture II and Conjecture III by providing an example which shows that the common technique used in proving Cohen's idempotent theorem, and several similar theorems, including some of our results in this thesis, is inherently inadequate for establishing these conjectures.

Chapter 2

Preliminaries

Let $\mathbb{D}$ denote the complex unit disk $\{z \in \mathbb{C} \mid |z| \leq 1\}$. For a positive integer n, we use $[n]$ to denote $\{1, \ldots, n\}$. For a set S we denote by $\mathbf{1}_S$ the indicator function of S. For a vector $x \in \{0,1\}^n$, and $S \subseteq [n]$, we denote by $x_S \in \{0,1\}^S$ the restriction of x to the coordinates in S. The Hamming weight of x is defined as $|x| \coloneqq \sum x_i$. For a matrix M its (i,j)-th entry is denoted by M_{ij} or $M(i,j)$.

All logarithms in this thesis are in base 2.

For two functions $f : \mathbb{N} \to \mathbb{R}$ and $g : \mathbb{N} \to \mathbb{R}$, we use the following asymptotic notations:

- $f(n) = O(g(n))$, if $\limsup\limits_{n\to\infty} \frac{|f(n)|}{|g(n)|} < \infty$.
- $f(n) = \Omega(g(n))$, if and only if $g(n) = O(f(n))$.
- $f(n) = \Theta(g(n))$, if $f(n) = O(g(n))$ and $f(n) = \Omega(g(n))$.
- $f(n) = o(g(n))$, if $\lim\limits_{n\to\infty} \frac{|f(n)|}{|g(n)|} = 0$.
- $f(n) = \omega(g(n))$, if $\lim\limits_{n\to\infty} \frac{|f(n)|}{|g(n)|} = \infty$.

We sometimes identify $\{0,1\}^n$ or $\mathbb{Z}_2^n$ with the vector space $\mathbb{F}_2^n$ over $\mathbb{F}_2$. In this context, we refer to cosets $H + a \subseteq \mathbb{Z}_2^n$ as affine subspaces, which naturally assign a dimensions and a codimension to them.

For sets $\mathcal{X}$ and $\mathcal{Y}$, we will often identify a function $f : \mathcal{X} \times \mathcal{Y} \to \mathbb{C}$ with its corresponding matrix $[f(x, y)]_{x\in\mathcal{X},y\in\mathcal{Y}}$.

For a measure space (Ω, μ), and $p \in [1, \infty)$, we denote by $L^p(\mu)$ the normed space of functions $f : \Omega \to \mathbb{C}$ with $\int |f|^p d\mu < \infty$, together with the norm

$$\|f\|_{L^p(\mu)} := \left(\int |f|^p d\mu\right)^{1/p},$$

and $\|f\|_{L^\infty(\mu)}$ is defined as the essential supremum of $|f|$.

For a *finite* set Ω, we write μ_Ω to denote the uniform probability measure on Ω, and we shorthand $\|f\|_{L^p(\mu_\Omega)}$ to $\|f\|_{L^p(\Omega)}$. When Ω is a countable set, we define the normed space $\ell_p(\Omega)$ according to the counting measure:

$$\|f\|_{\ell_p(\Omega)} = \left(\sum_{x\in\Omega} |f(x)|^p\right)^{1/p}.$$

There are several natural norms on the space of $m \times n$ matrices. Considering an $m \times n$ matrix M as a linear operator $M : \mathbb{C}^n \to \mathbb{C}^m$ endows the space with operator norms: For $p, q \in [1, \infty]$, we use the notation $\|M\|_{p\to q}$ to denote its operator norm from ℓ_p to ℓ_q. That is

$$\|M\|_{p\to q} = \sup_{x\in\mathbb{C}^n, \|x\|_{\ell_p}\le 1} \|Mx\|_{\ell_q},$$

It is easy to see that

$$\|M\|_{2\to 2} = \sigma_{\max},$$

where $\sigma_{\max}$ is the largest singular value of M.

We shall need the following well-known inequalities.

Lemma 2.1 (Hoeffding's inequality)**.** *For $i = 1, \ldots, n$, let X_i be independent random variables taking values from range $[a_i, b_i]$ and let $X = \sum_{i=1}^n X_i$. Then, for all $t > 0$,*

$$\Pr[|X - \mathbb{E}[X]| \ge t] < 2\exp\left(-\frac{2t^2}{\sum_i (b_i - a_i)^2}\right).$$

Lemma 2.2 (Cauchy–Schwarz inequality)**.** *Let u and v be arbitrary vectors of an inner product space over the field $\mathbb{C}$ or $\mathbb{R}$, then*

$$|\langle u, v\rangle| \le \|u\| \cdot \|v\|,$$

where the norm is induced by the inner product; $\|u\| = \sqrt{\langle u, u\rangle}$.

In particular, for the vectors u *and* v *from space* $\mathbb{R}^n$ *with dot product, the inequality has the following form:*

$$\left(\sum_{i=1}^{n} u_i v_i\right)^2 \leq \left(\sum_{i=1}^{n} u_i^2\right)\left(\sum_{i=1}^{n} v_i^2\right).$$

2.1 Communication complexity

2.1.1 Deterministic communication complexity

The field of communication complexity studies the amount of communication required to solve a problem of computing discrete functions when the input is split between two parties. In other words, communication complexity studies the following question:

How many bits need to be exchanged between two parties to evaluate the function?

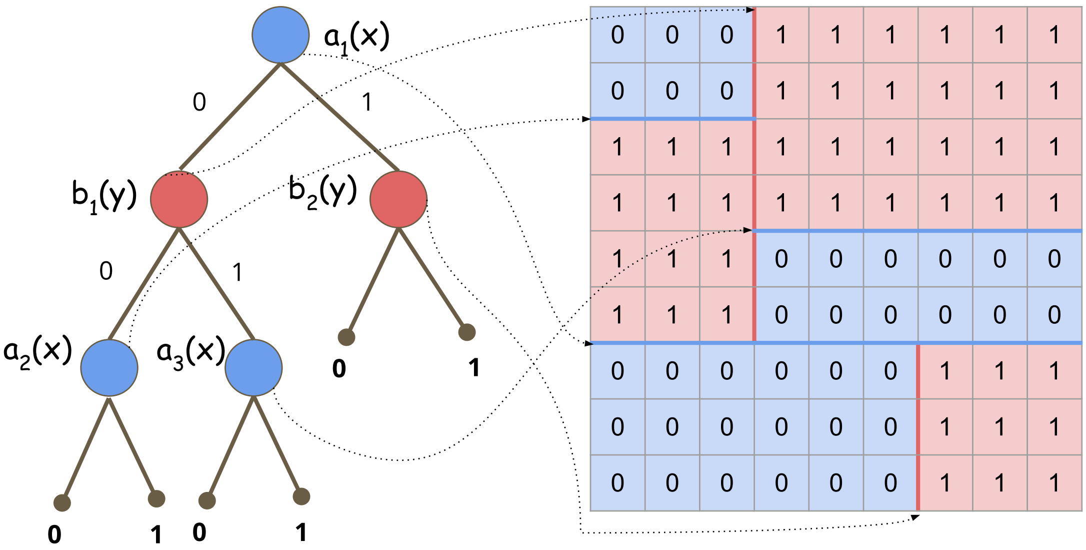
Every Boolean function $f : \mathcal{X} \times \mathcal{Y} \to \{0, 1\}$ defines a communication problem. An input $x \in \mathcal{X}$ is given to Alice, and an input $y \in Y$ is given to Bob. Together, they should both compute the entry $f(x, y)$ by exchanging bits of information in turn, according to a previously agreed-on protocol. There is no restriction on their computational power; the only measure we care to minimize is the number of exchanged bits.

A *deterministic* protocol π specifies for each of the two players, the bit to send next, as a function of their input and history of the communication so far. A protocol naturally corresponds to a binary tree as follows. Every internal node is associated with either Alice or Bob. If an internal node v is associated with Alice, then it is labeled with a function $a_v : \mathcal{X} \to \{0, 1\}$, which prescribes the bit sent by Alice at this node as a function of her input. Similarly, Bob's nodes are labeled with Boolean functions on $\mathcal{Y}$. Each leaf is labeled by 0 or 1 which corresponds to the output of the protocol. We denote the number of bits exchanged on the input (x, y) by $\mathrm{cost}_\pi(x, y)$. This is exactly the length of the path from the root to the corresponding leaf. The *communication cost* of the protocol is simply the depth of the protocol tree, which is the maximum of $\mathrm{cost}_\pi(x,y)$ over all inputs (x,y).

$$\mathrm{CC}(\pi) \coloneqq \max_{x,y} \mathrm{cost}_\pi(x,y).$$

Every such protocol π computes a function $\mathcal{X} \times \mathcal{Y} \to \{0,1\}$, which we also denote by π. Namely $\pi(x,y)$ is the label of the leaf reached by the path corresponding to the players' communication on the input (x,y). We say that π computes f if $\pi(x,y) = f(x,y)$ for all x, y. The *deterministic communication complexity* of f, denoted by $\mathrm{D}(f)$, is the smallest communication cost of a protocol that computes f.

A useful insight is that a bit sent by Alice at a node v corresponds to a partition of the rows into two parts $a_v^{-1}(0)$ and $a_v^{-1}(1)$, and every bit sent by Bob corresponds to a partition of the columns (see Figure 2.1). Every time Alice sends a bit, we restrict to a subset of the rows, and proceed with the created submatrix. Similarly Bob's communicated bits restrict the columns. As this process continues, we see that every c-bit protocol induces a partition of the matrix f into at most 2^c *submatrices* (see Figure 2.1). In the context of the communication complexity, submatrices are often called *combinatorial rectangles* or simply *rectangles*. If the protocol computes f, then all submatrices in this partition are *monochromatic*, namely, labeled by a unique element 0 or 1.



0	0	0	1	1	1	1	1	1
0	0	0	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1
1	1	1	0	0	0	0	0	0
1	1	1	0	0	0	0	0	0
0	0	0	0	0	0	1	1	1
0	0	0	0	0	0	1	1	1
0	0	0	0	0	0	1	1	1

Figure 2.1: A protocol tree on the left and its corresponding rectangle partitioning on the right.

Note that every rank-one Boolean matrix is of the form $\mathbf{1}_{\mathcal{X}_0} \cdot \mathbf{1}_{\mathcal{Y}_0}^T$ for subsets $\mathcal{X}_0 \subseteq \mathcal{X}$ and $\mathcal{Y}_0 \subseteq \mathcal{Y}$. Thus rank-one Boolean matrices are essentially the same as 1-monochromatic rectangles. We conclude the following proposition.

Proposition 2.3 ([KN97])**.** *For every Boolean matrix f, we have*

$$\log \mathrm{rk}(f) \leq \mathrm{D}(f) \leq \mathrm{rk}(f) \leq \mathrm{rk}(\mathscr{Rect}, f) \leq c \leq 2^{\mathrm{rk}(f)},$$

where c is the partition number *of f, which is the smallest $c > 0$ such that f can be partitioned into c constant submatrices. In particular, all the above parameters are qualitatively equivalent.*

To the extent that we are concerned with qualitative results, Proposition 2.3 provides a satisfactory description of the structure of Boolean matrices whose deterministic communication complexities are uniformly bounded. However, quantitatively, closing the exponential gap between $\mathrm{D}(f)$ and $\log \mathrm{rk}(f)$ into a polynomial dependency is called the log-rank conjecture, and is perhaps the most famous open problem in communication complexity [Lov14].

Conjecture 2.4 (Log-Rank Conjecture)**.** *There is an absolute constant $C > 0$ such that for every Boolean matrix f we have*

$$\mathrm{D}(f) \leq \log^{C}(\mathrm{rk}(f)).$$

2.1.2 Randomized communication complexity

In this thesis, we use the public coin model, where a *probabilistic protocol* π_R is simply a distribution over deterministic protocols. In this notation R is a random variable, and every fixation of R to a particular value r leads to a deterministic protocol π_r. We define the communication cost of a probabilistic protocol π_R as the maximum cost of any deterministic protocol π_r in the support of this distribution:

$$\mathrm{CC}(\pi_R) = \max_r \mathrm{CC}(\pi_r) = \max_r \max_{x,y} \mathrm{cost}_{\pi_r}(x,y).$$

We also define the *average cost* of such a protocol as the expected number of exchanged bits over the worst input (x, y):

$$\mathrm{CC}^{avg}(\pi_R) = \max_{x,y} \mathbb{E}_R[\mathrm{cost}_{\pi_R}(x,y)].$$

In the probabilistic models of computation, three types of error are often considered.

- **Two-sided error:** This is the most important notion of randomized communication complexity. For every x, y, we require

  $$\Pr_R[\pi_R(x,y) \neq f(x,y)] \leq \epsilon,$$

  where ϵ is a fixed constant that is strictly less than $1/2$. Note that $\epsilon = 1/2$ can be easily achieved by outputting a random bit; hence it is crucial that ϵ in the definition is strictly less than $1/2$. It is common to take $\epsilon = \frac{1}{3}$. Indeed, the choice of ϵ is not important so long as $\epsilon \in (0, 1/2)$, since the probability of error can be reduced to any constant $\epsilon' > 0$ by repeating the same protocol independently for some $O(1)$ times, and outputting the most frequent output (see Lemma 2.6).

The two-sided error communication complexity is simply called the *randomized communication complexity.* It is denoted by $\mathrm{R}_\epsilon(f)$ and is defined as the smallest communication cost $\mathrm{CC}(\pi_R)$ of a probabilistic protocol that computes f with two-sided error at most ϵ. We set $\epsilon = 1/3$ as the standard error, and denote

$$\mathrm{R}(f) = \mathrm{R}_{\frac{1}{3}}(f).$$

- **One-sided error:** In this setting the protocol is only allowed to make an error if $f(x,y) = 1$. In other words, for every x, y with $f(x,y) = 0$, we have

  $$\Pr_R[\pi_R(x,y) = 0] = 1,$$

  and for every x, y with $f(x,y) = 1$, we have

  $$\Pr_R[\pi_R(x,y) \neq f(x,y)] \leq \epsilon.$$

  Again the choice of ϵ is not important so long as $\epsilon \in (0,1)$ because the probability of error can be reduced from ϵ to ϵ^k by repeating the same protocol independently k times and outputting 1 only when at least one of the repetitions outputs 1. We denote by $\mathrm{R}^1_\epsilon(f)$ the smallest $\mathrm{CC}(\pi_R)$ over all protocols π_R with one-sided error of at most ϵ. We set $\epsilon = 1/3$ as the standard error, and denote

  $$\mathrm{R}^1(f) = \mathrm{R}^1_{\frac{1}{3}}(f).$$

- **Zero error:** In this case the protocol is not allowed to make any errors. For every x, y, we must have

  $$\Pr_R[\pi_R(x,y) \neq f(x,y)] = 0.$$

  In this setting, $\mathrm{CC}^{avg}(\cdot)$ is considered, as $\mathrm{CC}(\cdot)$ leads to the same notion of complexity as the deterministic communication complexity. We denote

  $$\mathrm{R}_0(f) = \inf \mathrm{CC}^{avg}(\pi_R),$$

  over all such protocols.

Note that one can convert a zero-error protocol π with average cost c to an one-sided error protocol π' with cost $3c$, by terminating the protocol after at most $3c$ steps, and outputting 0 in the case where the protocol is terminated prematurely. The protocol π' clearly does not make any errors on 0-inputs. Furthermore, since the average cost of π is c, by Markov's inequality, the probability that the protocol π' is terminated prematurely is at most $\frac{1}{3}$. We conclude

$$\mathrm{R}(f) \leq \mathrm{R}^1(f) \leq 3\,\mathrm{R}_0(f).$$

Obviously, $\mathrm{R}(f), \mathrm{R}^1(f), \mathrm{R}_0(f)$ are all upper-bounded by $\mathrm{D}(f)$.

Proposition 2.5. *For every Boolean matrix f, we have*

$$\mathrm{R}^1(f) = \Omega(\log C^1(f) - \log\log(n)), \tag{2.1}$$

where $C^1(f)$ is the 1-covering number *of f, which is the smallest $c > 0$ such that the 1's of f can be covered (possibly with intersections) by c all-one submatrices. In particular,*

$$\mathrm{R}_0(f) = \Omega\left(\log\bigl(C^1(f) + C^1(\overline{f})\bigr) - \log\log(n)\right).$$

To prove this we show that one-sided *private* randomized communication complexity of f is lower-bounded by $\log C^1(f)$, then Equation (2.1) will follow immediately from Newman's theorem (see Equation (1.5)). In contrast to public-coin randomized communication protocols, the private randomized protocol is defined as follows: Alice and Bob each get independent random strings r_A and r_B, the corresponding protocol is a binary tree where each of Alice's nodes are labeled by a function depending on x and r_A, and, similarly, Bob's nodes are labeled by functions depending on y and r_B. The input (x, y), as well as r_A and r_B, determine a leaf in the tree labeled by 0 or 1 – this label is the output of the protocol on input (x, y). Private randomized communication complexity of f is the height of the smallest tree computing f.

Proof of Proposition 2.5. Given the one-sided private randomized protocol π_R for f, take an input x, y such that $f(x, y) = 1$ and fix the random string $r = (r_A, r_B)$ for which $\pi_r(x, y) = 1$. For the fixed r let $S_r = \{(x, y) \colon \pi_r(x, y) = 1\}$. Note that S_r is a rectangle, and $f(x, y) = 1$

for all $(x,y) \in S_r$. Also note that for each (x,y) such that $f(x,y)=1$, there exists a random string r (or multiple strings) such that $(x,y) \in S_r$. Hence, the union of such rectangles covers all 1's of f. The number of 1-leaves in the tree is at most $2^{\mathrm{R}^1(f)}$, thus the number of rectangles, hence also $C^1(f)$, is at most $2^{\mathrm{R}^1(f)}$. □

For more extensive survey on these and other communication complexity models, we refer the interested reader to the books of Kushilevitz and Nisan [KN97], Jukna [Juk12], and Rao and Yehudayoff [RY20].

Error reduction

Lemma 2.6. *Let π be a randomized algorithm which computes the function $f : \mathcal{Z} \to \{0,1\}$ with error at most ϵ and complexity c. Then, for any $k > 0$, there is an algorithm π' computing f with error at most $2^{-\Omega\left(\left(\frac{1}{2}-\epsilon\right)^2 k\right)}$ and complexity $k \cdot c$.*

Proof. Define π' to run the algorithm π for k times independently and to output the most frequent answer. π' will output a wrong answer if π outputs incorrect answer more than $\frac{k}{2}$ times. For $i = 1, \dots, k$, let $X_i \in \{0,1\}$ denote the random variable which is 1 if the i-th run of π outputs a wrong answer, and is 0 otherwise. Then by the Hoeffding inequality (Lemma 2.1) for the upper tail:

$$\Pr\left[\sum_{i=1}^{k} X_i > \frac{k}{2}\right] \le 2\exp\left(-2\left(\frac{1}{2\epsilon}-1\right)^2 \cdot \frac{k^2\epsilon^2}{k}\right) = 2\exp\left(-2\left(\frac{1}{2}-\epsilon\right)^2 k\right).$$

□

2.2 Query complexity

In Section 2.1, we introduced various models of communication complexity. In this section we discuss query complexity. Let $\mathcal{X}$ be a finite set, often endowed with a product structure, most commonly $\mathcal{X} = \{0,1\}^n$. In query complexity, a function $f : \mathcal{X} \to \{0,1\}$ is fixed, and a player, who does not know the input x, wants to find out the value of $f(x)$ by making queries about x. In other words, query complexity strives to answer the following question:

How many queries to the input need to be done to evaluate the function?

The goal is to minimize the number of queries. Depending on what type of queries are allowed, we arrive at different models of query complexity. The most natural setting is to have $f : \{0,1\}^n \to \{0,1\}$. Denoting the input $x = (x_1, \ldots, x_n) \in \{0,1\}^n$, we consider three important types of queries, each leading to a different model of query complexity.

- The *coordinate queries* x_i for $i \in \{1, \ldots, n\}$.
- The *parity queries* $\oplus_{i \in S} x_i$, which are the XOR of the coordinates in S, for $S \subseteq [n]$.
- The AND *queries* $\prod_{i \in S} x_i$, for $S \subseteq [n]$.

Note that, similar to communication complexity, a protocol in each of these models corresponds to a binary tree where each internal node is labeled with a query, and the computation branches according to the output of these queries. The leaves are labeled with the output of the protocol. When only coordinate-queries are allowed, these trees are simply called *decision trees*. The *parity decision trees*, and AND-*decision trees*, respectively correspond to parity queries and AND queries.

The cost of such a protocol is the maximum number of queries made on an input, which is equal to the *depth* of the tree. Such trees naturally correspond to Boolean functions, and the *decision tree complexity* $\mathrm{dt}(f)$, the *parity decision tree complexity* $\mathrm{dt}^{\oplus}(f)$, and the AND-*decision tree complexity* $\mathrm{dt}^{\wedge}(f)$ are defined as the smallest depth required for the function f.

A randomized protocol is simply a distribution over deterministic protocols, and the notions of cost, average cost, zero-error, one-sided error, and two-sided error are defined analogous to communication complexity. The complexity measures corresponding to zero-error, one-sided error, and two-sided error are denoted respectively by rdt_0, rdt^1, rdt.

In the AND-query model, we denote these by $\mathrm{rdt}^{\wedge}_0$, $\mathrm{rdt}^{\wedge 1}$, $\mathrm{rdt}^{\wedge}$, and in the parity query model by $\mathrm{rdt}^{\oplus}_0$, $\mathrm{rdt}^{\oplus 1}$, $\mathrm{rdt}^{\oplus}$.

In the simple decision tree model of coordinate queries, a theorem of Nisan [Nis91] shows that all these parameters are qualitatively equivalent, in fact with polynomial dependencies.

Proposition 2.7 (Coordinate Query Equivalencies [Nis91]). *For every Boolean function $f : \{0,1\}^n \to \{0,1\}$, we have*

$$\operatorname{rdt}(f) \le \operatorname{rdt}^1(f) \le 3\operatorname{rdt}_0(f) \le 3\operatorname{dt}(f) \le 81\operatorname{rdt}(f)^2.$$

In light of Proposition 2.7, from the point of view of this thesis, the case of the coordinate query has been completely resolved. However, as we shall see later, in both the XOR and AND models, there are examples for which the randomized query complexity is $O(1)$, while the deterministic query complexity is $\Omega(n)$. We discuss the XOR-model in Chapter 5, and the AND-model in Chapter 6.

2.3 Lifting theorems: Communication versus Query

Communication to Query: Communication complexity is a more general model than query complexity, thus, intuitively, communication protocols are more powerful than decision trees. In fact, given a decision tree computing a function f and assuming the input to f is split between two parties Alice and Bob, one can obtain a communication protocol computing f by simulating the decision tree as follows: for a query to i-th input bit, the party who knows the i-th bit sends it to the other party, then the protocol proceeds to the next query in the decision tree. The number of bits transmitted by this communication protocol is equal to the number of queries required for the decision tree to compute f. It follows, lower bounds for communication complexity imply lower bounds for query complexity.

Query to Communication: This is the counter-intuitive direction – can restricted, weaker models simulate general, stronger models? In short, *lifting* theorems try to establish this direction as then lower bounds for the restricted model – which typically are easier to achieve – will imply lower bounds for the general model. In our context, lifting theorems transform an efficient communication protocol into an efficient decision tree, thus "lifting" lower bounds for decision trees into lower bounds for communication protocols.

The study of lifting theorems have been a very successful area of theoretical computer science, particularly in the past two decades [RM97, CKLM19, HHL18, GPW18a, GLM$^+$16, GPW20, GKPW17], resolving a wide range of problems in communication complexity, circuit complexity, proof complexity, data structures, etc.

Lifting theorems focus on *composed* functions: for a Boolean function $f : \{0,1\}^n \to \{0,1\}$ and $g : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$, the *lifted* function $F : \mathcal{X}^n \times \mathcal{Y}^n \to \{0,1\}$ is defined as

$$F\left((x_1, \ldots, x_n), (y_1, \ldots, y_n)\right) = f\left(g(x_1, y_1), \ldots, g(x_n, y_n)\right).$$

g is often called the *gadget* and f the *outer function*. Many interesting and well-studied functions in communication complexity fall into this setting such as Equality, set-disjointness, gap Hamming Distance and etc.. In this setting of composed functions the template of lifting theorems looks as follows:

Theorem 2.8 (Lifting theorem template)**.** *Let $\mathcal{C}^{\text{dt}}$ and $\mathcal{C}^{\text{CC}}$ be query complexity and communication complexity measures, respectively. Then,*

$$\mathcal{C}^{\text{CC}}(F) = \mathcal{C}^{\text{dt}}(f) \cdot \Theta(\mathcal{C}^{\text{CC}}(g)).$$

The choice of a gadget in lifting theorem plays a crucial role, its domain size should be small, though it can be non-constant. For example, let the gadget be the index function $\text{IND}_m : \{0,1\}^m \times [m] \to \{0,1\}$ on $m = \theta(n^c)$ bits, defined as $\text{IND}_m(x, i) = x_i$. Then [RM97] and [GPW20] showed that for any $f : \{0,1\}^n \to \{0,1\}$, the deterministic communication complexity of $F = f \circ \text{IND}_m^n$ is equivalent to f's decision tree complexity up to a $\log(n)$ factor, where $\log(n)$ in the upper bound is the communication complexity of IND_m. Consequently, lifting results with gadgets having non-constant domain size are going to give sub-optimal results, as we have to pay the communication cost of computing the gadget. So the ideal setting is when g's domain size is *constant*, i.e. $|\mathcal{X}| = |\mathcal{Y}| = O(1)$. We will focus on constant size gadgets in this thesis, in particular on the one-bit gadgets. The only non-equivalent one-bit gadgets are XOR and AND.

The framework that we are interested in this thesis is slightly different from as of above. Let G be a finite group. Every function $f : G \to \mathbb{C}$ defines a *lift* matrix

$$F : G \times G \to \mathbb{C}, \qquad F : (x, y) \mapsto f(y^{-1}x). \tag{2.2}$$

The XOR lift. The case of $G = \mathbb{Z}_2^n$ in (2.2) is closely related to the parity query complexity. The group operation on $\mathbb{Z}_2^n$ corresponds to the point-wise XOR operation on $\{0,1\}^n$, and hence for a given function $f : \{0,1\}^n \to \{0,1\}$, Equation (2.2) translates to $F_\oplus(x, y) = f(x \oplus y)$. The Fourier transform of f carries important information about the matrix $F_\oplus$. Indeed Fourier characters are the eigenvectors of $F_\oplus$, Fourier coefficients of f (scaled by the factor of 2^n) are their corresponding eigenvalues, and as a result

$$\mathrm{rk}(F_\oplus) = \mathrm{rk}_\oplus(f), \tag{2.3}$$

where $\mathrm{rk}_\oplus(f)$ denotes the number of non-zero Fourier coefficients of f.

The relation between parity query complexity parameters of f and their corresponding communication complexity parameters of $F_\oplus$ has been studied extensively [HHL18, TWXZ13, Zha14, ZS10, MS20, MO09].

Note that for $x, y \in \{0,1\}^n$,

$$\oplus_{i\in S}(x \oplus y)_i = (\oplus_{i\in S} x_i) \oplus (\oplus_{i\in S} y_i)\,,$$

which in particular allows one to translate every party decision tree to a communication protocol. Namely, every time that a query $\oplus_{i\in S}$ has been made in the parity decision tree, in the communication setting, the players can individually compute the two bits $\oplus_{i\in S} x_i$ and $\oplus_{i\in S} y_i$ and exchange them to find out the answer to the query on $x \oplus y$. It follows that $\mathrm{D}(F_\oplus), \mathrm{R}_0(F_\oplus), \mathrm{R}^1(F_\oplus)$, $\mathrm{R}(F_\oplus)$ are upper-bounded respectively by $2\,\mathrm{dt}^\oplus(f), 2\,\mathrm{rdt}_0^\oplus(f)$, $2\,\mathrm{rdt}^{\oplus 1}(f)$, $2\,\mathrm{rdt}^\oplus(f)$.

The difficult part of establishing a lifting theorem is indeed upper-bounding the query complexity in terms of the communication complexity. We will discuss these in Chapter 5.

The AND lift. In this case, we will work with the semigroup $(\{0,1\}^n, \wedge)$ where $\wedge$ corresponds to the pointwise product. Namely,

$$x \wedge y = (x_1 y_1, \dots, x_n y_n),$$

and the lifted function is defined as

$$F_\wedge(x, y) = f(x \wedge y).$$

Similar to the XOR setting, one easily shows that $\mathrm{D}(F_\wedge), \mathrm{R}_0(F_\wedge), \mathrm{R}^1(F_\wedge)$, $\mathrm{R}(F_\wedge)$ are upper-bounded respectively by $2\,\mathrm{dt}^\wedge(f), 2\,\mathrm{rdt}_0^\wedge(f), 2\,\mathrm{rdt}^{\wedge 1}(f)$, $2\,\mathrm{rdt}^\wedge(f)$. We will discuss the AND-lift in detail in Chapter 6.

2.4 Matrix norms and ranks

In this section we describe some well-known as well as some new matrix parameters which arise from representations of general matrices in terms of more structured matrices. Allowing $\mathcal{S}$ to be various sets of structured matrices (for example, $\mathcal{S} = \mathfrak{Rect}$ or $\mathcal{S} = \mathfrak{Blocky}$) we define, in a generic way, the matrix parameters that come up in this thesis. This also makes it easier to see how some of these parameters relate to each other. For a fixed set $\mathcal{S}$ of structured matrices, we introduce a notion of matrix *rank* in terms of $\mathcal{S}$, which we call $\mathcal{S}$-rank, and a matrix *norm* in terms of $\mathcal{S}$, which we call $\mathcal{S}$-norm analogously.

Definition 2.9. *Let $\mathcal{Z}$ be a* finite *set, and let $\mathcal{S}$ be a* spanning *subset of the vector space $\{f : \mathcal{Z} \to \mathbb{C}\}$.*

- *Define the $\mathcal{S}$-*rank *of a function f, denoted by $\mathrm{rk}(\mathcal{S}, f)$, to be the smallest k such that f can be expressed as a linear combination of at most k functions in $\mathcal{S}$ over $\mathbb{C}$.*
- *Define $\|f\|_\mathcal{S}$ as*

$$\|f\|_\mathcal{S} = \inf \left\{ \sum_{i=1}^r |\lambda_i| \ : \ f = \sum_{i=1}^r \lambda_i g_i, \ \textit{for } g_i \in \mathcal{S}, \lambda_i \in \mathbb{C}, r \in \mathbb{N} \right\}.$$

It is easy to verify that $\|\cdot\|_\mathcal{S}$ is always a semi-norm. By considering different $\mathcal{S}$ we can recover many of the norms and parameters related to this thesis.

- (*Normalized trace norm*) The *trace norm* of an $m \times n$ matrix M is defined as the sum of its singular values $\sigma_{\max} \coloneqq \sigma_1 \geq \ldots \geq \sigma_{\min(m,n)} \geq 0$, namely

$$\|M\|_{\mathrm{tr}} = \sum_{i=1}^{\min(m,n)} \sigma_i.$$

In this thesis, it is more convenient to work with the following normalized version of this norm, which we call the *normalized trace norm*:

$$\|M\|_{\mathrm{ntr}} = \frac{\|M\|_{\mathrm{tr}}}{\sqrt{mn}}.$$

When $\mathcal{S}$ is the set of all $m \times n$ matrices of the form $\mathbf{a} \otimes \mathbf{b}$, where $\mathbf{a} \in \mathbb{R}^m$ and $\mathbf{b} \in \mathbb{R}^n$ satisfy

$$\|\mathbf{a}\|_{L^2(m)} := \left(\sum_{i=1}^{m} \frac{|\mathbf{a}_i|^2}{m} \right)^{1/2} \leq 1, \text{ and } \|\mathbf{b}\|_{L^2(n)} := \left(\sum_{i=1}^{n} \frac{|\mathbf{b}_i|^2}{n} \right)^{1/2} \leq 1,$$

then $\mathrm{rk}(\mathcal{S}, M)$ coincides with $\mathrm{rk}(M)$ over $\mathbb{C}$, and it follows from the singular value decomposition theorem that

$$\|M\|_{\mathcal{S}} = \|M\|_{\mathrm{ntr}}.$$

- (*μ-norm*) If $\mathcal{S} = \mathcal{Rect}$, that is the set of rank-one Boolean matrices $\mathbf{a} \otimes \mathbf{b}$, where $\mathbf{a} \in \{0,1\}^m$ and $\mathbf{b} \in \{0,1\}^n$, then $\|\cdot\|_{\mathcal{Rect}}$ is commonly known as the $\|\cdot\|_\mu$ norm. Note that to define $\|\cdot\|_\mu$ one could equivalently take $\mathbf{a} \otimes \mathbf{b}$, where $\mathbf{a} \in [0,1]^m$ and $\mathbf{b} \in [0,1]^n$.

- (*ν-norm*) If $\mathcal{S}$ is the set of all $m \times n$ matrices of the form $\mathbf{a} \otimes \mathbf{b}$, where $\mathbf{a} \in \{-1,1\}^m$ and $\mathbf{b} \in \{-1,1\}^n$, then $\|\cdot\|_{\mathcal{S}}$ is commonly known as the $\|\cdot\|_\nu$ norm. Again to define $\|\cdot\|_\nu$ one could equivalently take $\mathbf{a} \otimes \mathbf{b}$, where $\mathbf{a} \in [-1,1]^m$ and $\mathbf{b} \in [-1,1]^n$.

  It immediately follows that $\|\cdot\|_\nu \leq \|\cdot\|_\mu$, but in fact the two norms are equivalent, since every $\{-1,1\}$-valued vector can be written as the difference of two Boolean vectors:

$$\|\cdot\|_\nu \leq \|\cdot\|_\mu \leq 4\|\cdot\|_\nu. \tag{2.4}$$

It will be useful to know that the identity matrix – an important example in the thesis – has constant ν-norm. Indeed, for the $n \times n$ identity matrix $\mathtt{I}_n$ we have

$$\mathtt{I}_n(x,y) = \frac{1}{2^n} \sum_{S \subseteq [n]} (-1)^{\sum_{i \in S} x_i} (-1)^{\sum_{i \in S} y_i},$$

and thus $\|\mathtt{I}_n\|_\nu = 1$.

- (γ_2-*norm*) We can relax the ν-norm further. Let $\mathcal{S}$ be the set of all $m \times n$ matrices with ij-entries $\langle \mathbf{a}_i, \mathbf{b}_j \rangle$, where $\mathbf{a}_i$ and $\mathbf{b}_j$ are *unit vectors* in any Hilbert space $\mathcal{H}$.

  Taking $\mathcal{H}$ to be $\mathbb{R}$, we have only two unit vectors ± 1 and thus we recover ν norm. Hence $\| \cdot \|_{\gamma_2} \leq \| \cdot \|_\nu$. It turns out that γ_2-norm is also equivalent to the ν norm. This is in fact the well-known Grothendieck inequality (see Theorem 2.10):

$$\| \cdot \|_{\gamma_2} \leq \| \cdot \|_\nu \leq \frac{\pi}{2\ln\left(1+\sqrt{2}\right)} \| \cdot \|_{\gamma_2}.$$

  The constant $\frac{\pi}{2\ln\left(1+\sqrt{2}\right)}$ is due to Krivine [Kri79], and it holds for both real and complex Hilbert spaces. Note also that the unit ball of $\| \cdot \|_{\gamma_2}$ is the set of $m \times n$ matrices with ij-entries $\langle \mathbf{a}_i, \mathbf{b}_j \rangle$, where $\|\mathbf{a}_i\| \leq 1$ and $\|\mathbf{b}_j\| \leq 1$ in some Hilbert space $\mathcal{H}$.

- (*Blocky-rank and norm*) For $\mathcal{S} = \mathcal{Blocky}$, we study $\mathrm{rk}(\mathcal{Blocky}, f)$, which we prove is qualitatively equivalent to the deterministic communication complexity with access to equality oracle (see Proposition 4.1). We refer to $\| \cdot \|_{\mathcal{Blocky}}$ as *blocky-norm*. Blocky matrices are the blow-ups of the identity matrix, and thus every non-zero blocky matrix B satisfies

$$\|B\|_{\gamma_2} = \|B\|_\nu = 1.$$

  On the other hand, every $\mathbf{a} \otimes \mathbf{b}$, where $\mathbf{a} \in \{-1, 1\}^m$ and $\mathbf{b} \in \{-1, 1\}^n$, can be written as the difference of two blocky matrices, and thus satisfies $\|\mathbf{a} \otimes \mathbf{b}\|_{\mathcal{Blocky}} \leq 2$. We conclude

$$\| \cdot \|_\nu \leq \| \cdot \|_{\mathcal{Blocky}} \leq 2 \| \cdot \|_\nu. \tag{2.5}$$

  Combining this with Equation (2.4) and with the fact that a rank-one Boolean matrix is also a blocky matrix, we deduce:

$$\frac{1}{4} \| \cdot \|_\mu \leq \| \cdot \|_{\mathcal{Blocky}} \leq \| \cdot \|_\mu. \tag{2.6}$$

- (*Fourier rank and algebra norm*) Let G be a finite Abelian group with dual $\widehat{G}$. Then for $f : G \to \mathbb{C}$,

$$\mathrm{rk}(\widehat{G}, f)$$

corresponds to the so-called *Fourier rank* of f, which is the number of non-zero Fourier coefficients of f. In this case, the corresponding norm coincides with Fourier algebra norm

$$\|f\|_{\widehat{G}} = \|f\|_A.$$

- (*Monomial rank and norm*) Consider the space of functions $f : \{0,1\}^n \to \mathbb{C}$, and let

  $$\mathcal{M}on := \left\{ x \mapsto \prod_{i \in S} x_i \mid S \subseteq [n] \right\}$$

  be the set of all monomials where every variable appears with degree at most 1. Then, for a function $f : \{0,1\}^n \to \mathbb{C}$,

  $$\mathrm{rk}(\mathcal{M}on, f)$$

  corresponds to the number of non-zero coefficients in the (unique) polynomial representation of f. This is often called the *sparsity* of f in the literature of computer science. Note also that $\|f\|_{\mathcal{M}on}$ is the sum of absolute value of the coefficients in the unique polynomial representation of f in the ring $\mathbb{C}[x_1, \ldots, x_n]/(x_1^2 = x_1, \ldots, x_n^2 = x_n)$.

Schur Multipliers Let $\mathcal{X}$ and $\mathcal{Y}$ be two countable sets. The *Schur product*, also known as the *Hadamard product* of two $\mathcal{X} \times \mathcal{Y}$ matrices $A = [a_{xy}]$ and $B = [b_{xy}]$, denoted by $A \circ B$, is their entry-wise product $[a_{xy} \cdot b_{xy}]$. Consider the two Hilbert spaces $\mathcal{H}_1 = \ell_2(\mathcal{Y})$ and $\mathcal{H}_2 = \ell_2(\mathcal{X})$, and let $B(\mathcal{H}_1, \mathcal{H}_2)$ be the space of all *bounded* linear operators $A : \mathcal{H}_1 \to \mathcal{H}_2$ together with the operator norm $\|A\|_{\mathcal{H}_1 \to \mathcal{H}_2}$. We correspond the linear operator $A : \mathcal{H}_1 \to \mathcal{H}_2$ to an $\mathcal{X} \times \mathcal{Y}$ matrix. A matrix $M_{\mathcal{X} \times \mathcal{Y}}$ is called a *Schur multiplier* if for every $A \in B(\mathcal{H}_1, \mathcal{H}_2)$, the matrix $M \circ A \in B(\mathcal{H}_1, \mathcal{H}_2)$. Every Schur multiplier defines a map $B(\mathcal{H}_1, \mathcal{H}_2) \to B(\mathcal{H}_1, \mathcal{H}_2)$ via $A \mapsto M \circ A$.

To distinguish from the norm on bounded operators, we will write $\|M\|_m$ for the *norm of a Schur multiplier*:

$$\|M\|_m = \sup\{\|M \circ A\|_{\mathcal{H}_1 \to \mathcal{H}_2} \ : \ \|A\|_{\mathcal{H}_1 \to \mathcal{H}_2} \leq 1\}.$$

It turns out that $\|\cdot\|_m$ coincides with γ_2 norm defined above. The following relations are essentially due to Grothendieck (see also [LS07, Pis12]).

Theorem 2.10 (Grothendieck [Gro52])**.** *For every matrix M,*

$$\|M\|_m = \|M\|_{\gamma_2} \leq \|M\|_\nu \leq \frac{\pi}{2\ln\bigl(1+\sqrt{2}\bigr)}\|M\|_{\gamma_2}.$$

For the proof of the first equality, we refer the reader to [Pis12, Proposition 3.3]. In other words, $\|\cdot\|_m$, $\|\cdot\|_\mu$, $\|\cdot\|_\nu$, and $\|\cdot\|_{\gamma_2}$ are all within constant factors of each other. Let us also mention the following common properties of $\|\cdot\|_m$ and $\|\cdot\|_{\gamma_2}$ norm.

Proposition 2.11. *Let M_i be a sequence of matrices. Then the following holds for their direct sum*

$$\|\oplus_{i=1}^{\infty} M_i\|_m = \sup_i \|M_i\|_m.$$

In particular, the equality also holds for $\|\cdot\|_{\gamma_2}$.

Proof. First note that $\|\oplus_{i=1}^{\infty} M_i\|_m \geq \sup_i \|M_i\|_m$ as the operator norm does not increase under restriction.

For the other direction, denote $M = \oplus_{i=1}^{\infty} M_i$, and let M_i' be the extension of M_i such that it has the dimensions of M and is all-zero outside of M_i. From the definition of $\|\cdot\|_m$ there is a matrix A such that $\|A\|_{\mathcal{H}_1\to\mathcal{H}_2} = 1$ and $\|M\|_m = \|M \circ A\|_{\mathcal{H}_1\to\mathcal{H}_2}$. Given A, we can deduce

$$\|M\|_m = \|M \circ A\|_{\mathcal{H}_1\to\mathcal{H}_2} = \sup_i \|M_i' \circ A\|_{\mathcal{H}_1\to\mathcal{H}_2} \leq \sup_i \|M_i'\|_m = \sup_i \|M_i\|_m.$$

Here the second equality is a property of operator norm, which is straightforward to verify.

□

Proposition 2.12. *For a matrix $M_{\mathcal{X}\times\mathcal{Y}} = [m_{ij}]$, $\|M\|_m \leq 1$ if and only if there exist vectors $x_1, \ldots, x_{|\mathcal{X}|}$ and $y_1, \ldots, y_{|\mathcal{Y}|}$ from the unit ball of some Hilbert space $\mathcal{H}$ such that $\langle x_i, y_j\rangle = m_{ij}$.*

We refer the reader to [Pau02, Theorem 8.7] or [Pis96, Theorem 5.1] for the proof.

Idempotents and Boolean matrices Schur multipliers on $B(\mathcal{H}_1, \mathcal{H}_2)$ form a Banach algebra via the Schur product, since

$$\|M_1 \circ M_2\|_m \leq \|M_1\|_m \|M_2\|_m.$$

When $\mathcal{H}_1$ and $\mathcal{H}_2$ are finite dimensional, Boolean matrices and *idempotents* of this algebra coincide: $M \circ M = M$ if and only if M is a Boolean matrix. However, in the infinite dimensions, not every Boolean matrix is a bounded Schur multiplier.

We will be interested in characterizing the idempotents of the algebra of Schur multipliers. As we shall see in Theorem 4.12, this reduces to characterizing the structure of finite Boolean matrices M with a uniform bound on $\|M\|_m$.

First let us consider the contractive idempotents. Note that every rank-one Boolean matrix is a contraction. As a result, by Proposition 2.11, the identity matrix and, more generally, all blocky matrices are contractions.

Note that the Schur multiplier norm is monotone in the sense that the norm of a submatrix cannot be larger than the original matrix. Since $\|1\|_m = 1$, it follows that every non-zero Boolean matrix satisfies $\|M\|_m \geq 1$. Livshits [Liv95] showed that the 2×2 matrix with three 1's is not contractive.

Lemma 2.13 ([Liv95])**.** *We have*

$$\left\| \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\|_m = \frac{2}{\sqrt{3}} > 1.$$

Since $\|\cdot\|_m$ norm is invariant under row and column permutations, it follows that a contractive idempotent M cannot have any 2×2 submatrices with exactly 3 ones. In this context, the property is often called the 3-*of*-4 *property*, which fully characterizes such matrices as being the same as the set of *blocky*-matrices.

Theorem 2.14 ([Liv95])**.** *M is a contractive idempotent of the algebra of Schur multipliers if and only if $M \in \mathscr{Blocky}$. More generally, this is true for idempotents that satisfy $\|M\|_m < \frac{2}{\sqrt{3}}$.*

Relation to the Normalized Trace Norm As we saw above $\|\cdot\|_{\gamma_2} = \|\cdot\|_m$, $\|\cdot\|_\mu$, and $\|\cdot\|_\nu$, are all equivalent. Furthermore, it is easy to see [LS07, Section 2.3.2] that

$$\|\cdot\|_{\mathrm{ntr}} \leq \|\cdot\|_{\gamma_2}. \tag{2.7}$$

However, $\|\cdot\|_{\mathrm{ntr}}$ could be much smaller than the above norms since adding all-zero rows or columns would decrease the normalized trace norm, while other norms would remain intact.

2.4.1 The Fourier algebra norm

Let $f : \{0,1\}^n \to \{0,1\}$ be a Boolean function. Identifying $\{0,1\}^n$ with the finite Abelian group $G = \mathbb{Z}_2^n$ allows us to consider the Fourier expansion of $f = \sum_{\chi \in \widehat{G}} \hat{f}(\chi)\chi$, where $\widehat{G}$ is the dual of G and its elements χ are called *characters* of G. It is common in theoretical computer science to represent this expansion as

$$f = \sum_{S \subseteq [n]} \hat{f}(S)\chi_S,$$

by representing the characters of $\mathbb{Z}_2^n$ as

$$\chi_S : x \mapsto \prod_{i \in S} (-1)^{x_i}.$$

The Fourier algebra norm of f, denoted by $\|f\|_A$, is the sum of absolute values of Fourier coefficients:

$$\|f\|_A = \sum_S |\widehat{f}(S)|.$$

The name comes from the fact that it satisfies $\|f_1 f_2\|_A \le \|f_1\|_A \|f_2\|_A$ for any $f_1, f_2 : G \to \mathbb{C}$. In the literature of theoretical computer science, this norm is sometimes called the *spectral norm* of f, but in order to avoid confusion with spectral norm of matrices, we will use the harmonic analysis term, *Fourier algebra norm.*

The above definition immediately generalizes to every finite Abelian group G, namely the Fourier algebra norm of $f : G \to \mathbb{C}$ is the sum of absolute values of Fourier coefficients. This can be further generalized to every locally compact Abelian group, and in fact Eymard in [Eym64] generalized the definition of the Fourier algebra to every locally compact group. In this thesis, we are only concerned with finite groups. Suppose that G is a finite group and $f, g : G \to \mathbb{C}$. The convolution $f * g$ of f and g is then defined point-wise by

$$f * g(x) \coloneqq \mathbb{E}_{y \in G} \left[f(y) g(y^{-1}x) \right]. \tag{2.8}$$

This can be used to introduce the *convolution operator*: given $h : G \to \mathbb{C}$, define $L_h : L^2(G) \to L^2(G)$ via $L_h : \nu \mapsto \nu * h$. The Fourier algebra norm of f is then defined as

$$\|f\|_A \coloneqq \sup \left\{ \langle f, h \rangle \ : \|L_h\|_{L^2(G) \to L^2(G)} \le 1 \right\}.$$

When G is an *Abelian* group, it is not difficult to see that this coincides with the sum of absolute values of Fourier coefficients of f:

$$\|f\|_A = \sum_{\chi \in \widehat{G}} |\widehat{f}(\chi)|.$$

2.5 Approximate norms and randomized complexity, a general approach

The study of randomized complexity classes is often naturally linked to approximate norms. For every matrix norm $\|\cdot\|$ and every $\epsilon > 0$, we define a corresponding ϵ-approximate norm for *real* matrices M as

$$\|M\|_\epsilon = \inf\{\|N\| \ : \ |M(x,y) - N(x,y)| \leq \epsilon \ \ \forall x, y\},$$

where in the infimum N is a real matrix of the same dimensions as M.

Similarly, for every norm $\|\cdot\|$ on the space of *real-valued* functions $f : \mathcal{X} \to \mathbb{R}$, we define the ϵ-approximate version of the norm as

$$\|f\|_\epsilon = \inf\{\|g\| \ : \|f - g\|_\infty \leq \epsilon, \ g : \mathcal{X} \to \mathbb{R}\}.$$

We also define the notion of the approximate $\mathcal{S}$-rank similarly:

$$\mathrm{rk}_\epsilon(\mathcal{S}, f) = \min\{\mathrm{rk}(\mathcal{S}, g) \ : \|f - g\|_\infty \leq \epsilon, \ g : \mathcal{X} \to \mathbb{R}\},$$

where we are using the notation of Definition 2.9.

We use $\mathrm{rk}_\epsilon(M)$ to denote the ϵ-rank of a real matrix M, which is the minimum rank over real matrices that approximate every entry of M to within an additive ϵ. Similar to randomized complexity measures, the choice of ϵ is not very important, as changing ϵ could only affect the value of the approximate-rank of a Boolean matrix polynomially [KS07].

Approximate norms and randomized protocols, a general approach. Suppose we are given a function $f : \mathcal{Z} \to \{0,1\}$, and we are interested in complexity of f in a randomized model of computation $\mathcal{M}$. Here $\mathcal{M}$ could be the communication complexity model, in which case we think of $\mathcal{Z} = \mathcal{X} \times \mathcal{Y}$, or any of the query complexity models discussed above, in which case $\mathcal{Z} = \{0,1\}^n$.

Consider also the set of all the deterministic (query or communication) protocols π, each computing a corresponding function $\pi : \mathcal{Z} \to \{0,1\}$. Furthermore, the cost of every deterministic protocol π, denoted by $\mathrm{cost}(\pi) \in \mathbb{N}$, is the worst-case number of queries or communicated bits used by the protocol over the set of all inputs. This defines the deterministic complexity of a function f as

$$\mathrm{D}^{\mathcal{M}}(f) \coloneqq \inf\{\mathrm{cost}(\pi) : \pi(z) = f(z)\ \forall z \in \mathcal{Z}\}.$$

A randomized protocol π_R is a probability distribution over deterministic protocols π_r, and the cost of a randomized protocol is defined to be the maximum cost of a deterministic protocol in its support. This leads to the notion of the randomized complexity of a function f:

$$\mathrm{R}^{\mathcal{M}}_{\epsilon}(f) \coloneqq \inf\{\mathrm{cost}(\pi_R) : \Pr_R[\pi_R(z) \neq f(z)] \leq \epsilon\ \forall z \in \mathcal{Z}\}.$$

The following lemma provides a connection between the randomized complexity and a suitable notion of approximate norm.

Lemma 2.15 (Equivalence of $\mathrm{R}^{\mathcal{M}}_{\epsilon}(f)$ and $\|f\|_{\mathcal{S},\epsilon}$)**.** *Consider the setting described above. Let $\mathcal{S}$ be a spanning subset of functions $\mathcal{Z} \to \mathbb{D}$, and $\epsilon \in (0, \frac{1}{2})$ be a parameter.*

(i) If there exists an increasing function $\kappa : \mathbb{R}^+ \to \mathbb{R}^+$ such that for every function $f : \mathcal{Z} \to \{0,1\}$,

$$\|f\|_{\mathcal{S}} \leq \kappa(\mathrm{D}^{\mathcal{M}}(f)),$$

then

$$\|f\|_{\mathcal{S},\epsilon} \leq \kappa(\mathrm{R}^{\mathcal{M}}_{\epsilon}(f)).$$

(ii) If every $h \in \mathcal{S}$ satisfies

$$\mathrm{D}^{\mathcal{M}}(h) \leq c,$$

then

$$\mathrm{R}_{\epsilon}^{\mathcal{M}}(f) \leq \frac{32c\log(2/\epsilon)}{(1-2\epsilon)^2}\|f\|_{\mathcal{S},\epsilon}^2.$$

Proof. (i) Consider a randomized protocol π_R of cost at most c that computes f with two-sided error at most ϵ. Then

$$\|\mathbb{E}_R[\pi_R] - f\|_\infty \leq \epsilon,$$

while by convexity

$$\|f\|_{\mathcal{S},\varepsilon} \leq \|\mathbb{E}_R[\pi_R]\|_{\mathcal{S}} \leq \mathbb{E}_R\left[\|\pi_R\|_{\mathcal{S}}\right] \leq \max_r \|\pi_r\|_{\mathcal{S}}$$

$$\leq \max_r \kappa(\mathrm{D}^{\mathcal{M}}(\pi_r)) \leq \max_r \kappa(\mathrm{cost}(\pi_r)) = \kappa(\mathrm{R}_{\epsilon}^{\mathcal{M}}(f)), \quad (2.9)$$

as desired.

(ii) Let $\delta = \frac{1-2\epsilon}{4}$. Recall that the approximate norm $\|f\|_{\mathcal{S},\epsilon}$ is defined as the infimum of $\|f'\|_{\mathcal{S}}$ such that $\|f - f'\|_\infty \leq \epsilon$, however, there might not exist a function f' witnessing the infimum. Hence, instead let $\lambda_i \in \mathbb{C}$ and $h_i \in \mathcal{S}$ be such that $f' = \sum_{i=1}^k \lambda_i h_i$ satisfies $\|f - f'\|_\infty \leq \epsilon + \delta$, and

$$L := \sum_{i=1}^k |\lambda_i| \leq \|f\|_{\mathcal{S},\epsilon}.$$

We will convert this to a randomized protocol.

For every i, define $\lambda_i' := \frac{\lambda_i}{|\lambda_i|}$, so that $|\lambda_i'| = 1$. Pick g randomly from $\{\lambda_1' h_1, \ldots, \lambda_k' h_k\}$ according to the probability distribution

$$\Pr[g = \lambda_i' h_i] = \frac{|\lambda_i|}{\sum_{i=1}^k |\lambda_i|}.$$

Note that $\mathbb{E}[g] = f'/L$, and furthermore $\|g\|_\infty \leq 1$ by our assumption about $\mathcal{S}$. Let $N = 2\delta^{-2}L^2\log(2/\epsilon) = \frac{32L^2\log(2/\epsilon)}{(1-2\epsilon)^2}$, and $g_1, \ldots, g_N$ be i.i.d. copies of g, and define $\widetilde{G} = \frac{L}{N}\sum_{i=1}^N g_i$. For every $z \in \mathcal{Z}$, by applying Hoeffding's inequality (Lemma 2.1) to the real part of $\widetilde{G}$, we have

$$\Pr\left[|\,\mathrm{re}(\widetilde{G}(z)) - \mathrm{re}(f'(z))| \geq \delta\right] < 2\exp\left(-\frac{2\delta^2}{4N\cdot(L/N)^2}\right) \leq \epsilon,$$

where the last inequality is by the choice of N. Next, let G be the Boolean rounding of $\widetilde{G}$, that is $G(z) = 1$ if and only $\mathrm{re}(\widetilde{G}(z)) \geq 1/2$. Noting that $|\,\mathrm{re}(f'(z)) - f(z)| \leq \epsilon + \delta$, we have

$$\Pr[G(z) \neq f(z)] \leq \Pr\left[|\,\mathrm{re}(\tilde{G}(z)) - \mathrm{re}(f'(z))| \geq \frac{1}{2} - \epsilon - \delta\right]$$

$$\leq \Pr\left[|\,\mathrm{re}(\widetilde{G}(z)) - \mathrm{re}(f'(z))| \geq \delta\right] \leq \epsilon. \quad (2.10)$$

Note that by our assumption each h_i can be computed at cost at most c. Since $\tilde{G}(z)$ can be computed by rounding a linear combination of N such h_i's, it can be computed at cost cN. This concludes the statement. □

Next we apply Lemma 2.15 to specific models of query and communication complexity.

Corollary 2.16. *For $\epsilon > 0$, let $c_\epsilon = \frac{\log(1/\varepsilon)}{(1-2\epsilon)^2}$. We have*

(a) AND*-query model:*

$$\log_3 \|f\|_{\mathcal{M}on,\varepsilon} \leq \mathrm{rdt}^{\wedge}_{\varepsilon}(f) \leq O\left(c_\epsilon \cdot \|f\|^2_{\mathcal{M}on,\varepsilon}\right).$$

(b) XOR*-query model:*

$$\log_2 \|f\|_{A,\varepsilon} \leq \mathrm{rdt}^{\oplus}_{\epsilon}(f) \leq O\left(c_\epsilon \cdot \|f\|^2_{A,\varepsilon}\right).$$

(c) Randomized communication complexity:

$$\log_2 \|F\|_{\mu,\varepsilon} \leq \mathrm{R}_\epsilon(F) \leq O\left(c_\epsilon \cdot \|F\|^2_{\mu,\varepsilon}\right),$$

which, in particular, implies

$$\log_2 \|F\|_{\gamma_2,\varepsilon} \leq \mathrm{R}_\epsilon(F) \leq O\left(c_\epsilon \cdot \|F\|^2_{\gamma_2,\varepsilon}\right),$$

Proof. (a) AND-query model: $\mathcal{Z} = \{0,1\}^n$, and $\mathcal{S} = \mathcal{M}on$.

Later in Proposition 6.1, we will prove that $\|f\|_{\mathcal{M}on} \leq 3^{\mathrm{dt}^{\wedge}(f)}$. Hence the lower bounds follows from Lemma 2.15 (i).

The upper bound follows directly from Lemma 2.15 (ii), as for every $h_S \coloneqq \prod_{i \in S} x_i \in \mathcal{M}on$, $\mathrm{dt}^{\wedge}(h_S) = 1$.

(b) XOR-query model: $\mathcal{Z} = \{0,1\}^n$, and $\mathcal{S} = \{\chi_S\}_{S\subseteq[n]}$, the set of characters of $\mathbb{Z}_2^n$.

By Cauchy-Schwarz inequality (Lemma 2.2) $\|f\|_A \leq \sqrt{\mathrm{rk}_\oplus(f)} \cdot \|f\|_{L^2(\mathcal{Z})} \leq \sqrt{\mathrm{rk}_\oplus(f)}$, which combined with Proposition 5.1 below, gives $\|f\|_A \leq 2^{\mathrm{dt}^\oplus(f)}$. Now Lemma 2.15 (i) yields the lower bound.

The upper bound follows from Lemma 2.15 (ii), noting that $\mathrm{dt}^\oplus(\chi_S) = 1$ for all $S \subseteq [n]$.

(c) Randomized Communication Complexity: $\mathcal{Z} = \mathcal{X} \times \mathcal{Y}$, $\mathcal{S} = \mathscr{Rect}$.

A communication protocol of cost c provides a partition of F into at most 2^c monochromatic rectangles, and thus $\|F\|_\mu \leq 2^{\mathrm{D}(F)}$. Now the lower bound follows from Lemma 2.15 (i).

The upper bound follows from Lemma 2.15 (ii) by noting that $\mathrm{D}(h) = O(1)$ for every $h \in \mathscr{Rect}$.

□

2.6 Communication Complexity Classes and Conjecture I

Babai, Frankl, and Simon [BFS86] introduced the hierarchy of communication complexity classes inspired by classical complexity theory classes where the model of computation is the Turing machine. Though since then, there has been a lot of research on this topic, there are still numerous open questions and unknown relationships between classes. One of the motivations behind Conjecture I, as we explain below, stems from the open question of separating classes $\mathbf{BPP}^{\mathrm{CC}}$ and $\mathbf{P}^{\mathbf{NP}^{\mathrm{CC}}}$.

Göös, Pitassi and Watson in [GPW18b] surveyed the known relationships adding some new results as well. Here we will bring the definitions of only those classes which we need. For the complete list refer to [GPW18b]. We define the classes on the universe of functions $f : \{0,1\}^{\log n} \times \{0,1\}^{\log n} \to \{0,1\}$ or equivalently, $n \times n$ matrices.

- $\mathbf{P}^{\mathrm{CC}}$ is the set of those functions for which there exists a *deterministic* communication protocol solving it with cost $\log^c(\log n)$, for some constant $c > 0$.

- $\mathbf{NP}^{\mathrm{CC}}$ is the set of functions that can be solved by a *non-deterministic* communication protocol of $\log^c(\log n)$ cost, for some constant $c > 0$. Non-deterministic communication complexity of a function f is equal to the logarithm of 1-covering number of f, which is the smallest $k > 0$ such that the 1's of f can be covered (possibly with intersections) by k all-one submatrices.

- $\mathbf{BPP}^{\mathrm{CC}}$ is the set of functions f such that can be solved by a *public-coin randomized* communication protocol of $\log^c(\log n)$ cost, for some constant $c > 0$.

- $\mathbf{PP}^{\mathrm{CC}}$ is the set of functions f that for some constant $c > 0$ have $\log^c(\log n)$ *weakly unbounded-error randomized complexity* , which is defined by $\inf_{0\leq\epsilon\leq 1/2}\left\{\mathrm{R}_\epsilon(f) + \log\left(\frac{1}{1-2\epsilon}\right)\right\}$. This includes an additional penalty term, which increases as ϵ approaches 1/2.

- $\mathbf{P}^{\mathrm{EQ}^{\mathrm{CC}}}$ is the set of functions f that for some constant $c > 0$ can be solved by a deterministic protocol of cost $\log^c(\log n)$ which has access to an oracle solving the Equality problem (i.e. the identity matrix) and each query to the oracle costs 1 extra bit. The complexity of such protocols is denoted by $\mathrm{D}^{\mathrm{EQ}}(f)$.

- $\mathbf{P}^{\mathbf{NP}^{\mathrm{CC}}}$ is the set of functions that, for some constant $c > 0$, can be solved by a deterministic protocol of cost $\log^c(\log n)$ which has access to an oracle solving problems from $\mathbf{NP}^{\mathrm{CC}}$ and is charged an extra 1 bit for each query to the oracle. Obviously, $\mathbf{P}^{\mathrm{EQ}^{\mathrm{CC}}} \subset \mathbf{P}^{\mathbf{NP}^{\mathrm{CC}}}$.

However, unlike classical complexity theory, most of the relationships between these classes are already known (Figure 2.2.).

As stated in [CLV19], one of the reasons to study Conjecture I is an old open question of [BFS86] (stated explicitly in [GPW18b]): Is $\mathbf{BPP}^{\mathrm{CC}} \subseteq \mathbf{P}^{\mathbf{NP}^{\mathrm{CC}}}$ for total functions?

It is known that $\mathbf{BPP}^{\mathrm{CC}} \neq \mathbf{P}^{\mathbf{NP}^{\mathrm{CC}}}$, since $\mathbf{BPP}^{\mathrm{CC}} \subset \mathbf{PP}^{\mathrm{CC}}$, while $\mathbf{P}^{\mathbf{NP}^{\mathrm{CC}}} \not\subseteq \mathbf{PP}^{\mathrm{CC}}$. Or, simply note that the Set-Disjointness function is not in $\mathbf{BPP}^{\mathrm{CC}}$, but it is in $\mathbf{P}^{\mathbf{NP}^{\mathrm{CC}}}$.

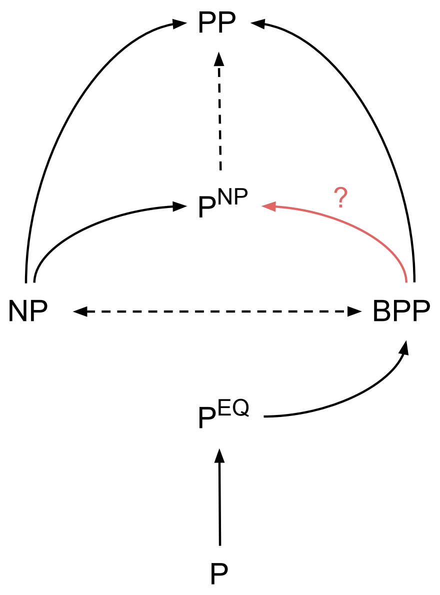


Figure 2.2: $C_1 \rightarrow C_2$ denotes $C_1 \subseteq C_2$, and $C_1 \dashrightarrow C_2$ denotes $C_1 \not\subseteq C_2$, Red indicates the open problem we are interested in.

Interestingly, there is a *partial* function – a function defined only on a subset of inputs – separating $\mathbf{BPP}^{\mathrm{CC}}$ and $\mathbf{P}^{\mathbf{NP}^{\mathrm{CC}}}$ (a version of Gap-Hamming-Distance function [PSS14]). However, there is no known *total* function separating $\mathbf{BPP}^{\mathrm{CC}}$ and $\mathbf{P}^{\mathbf{NP}^{\mathrm{CC}}}$. [CLV19] showed a separation between $\mathbf{BPP}^{\mathrm{CC}}$ and $\mathbf{P}^{\mathrm{EQ}^{\mathrm{CC}}}$ – one of the most interesting subclasses of $\mathbf{P}^{\mathbf{NP}^{\mathrm{CC}}}$. While this was an important milestone, the question whether $\mathbf{BPP}^{\mathrm{CC}} \not\subseteq \mathbf{P}^{\mathbf{NP}^{\mathrm{CC}}}$ remains open.

A result of [PSS14] suggests that Conjecture I stands as a barrier for understanding the relation between $\mathbf{BPP}^{\mathrm{CC}}$ and $\mathbf{P}^{\mathbf{NP}^{\mathrm{CC}}}$. [PSS14] showed that a matrix F has a $\mathbf{P}^{\mathbf{NP}^{\mathrm{CC}}}$ protocol of cost c if and only if there exists a list of 2^c tuples (R_i, z_i), where R_i is a submatrix of F and $z_i \in \{0,1\}$, such that $F(x,y) = z_i$ for the first submatrix R_i in the list for which $(x,y) \in R_i$. Having this, if $\mathbf{BPP}^{\mathrm{CC}} \subset \mathbf{P}^{\mathbf{NP}^{\mathrm{CC}}}$, then for all $F \in \mathbf{BPP}^{\mathrm{CC}}$ it is not hard to verify that there exists an all-one or all-zero submatrix in F of density $2^{-O(c)}$ for $c = \mathrm{polylog}(\log n)$. Thus, refuting Conjecture I, will show that $\mathbf{BPP}^{\mathrm{CC}} \not\subseteq \mathbf{P}^{\mathbf{NP}^{\mathrm{CC}}}$. On the other hand, if Conjecture I is true, it will suggest a positive evidence towards $\mathbf{BPP}^{\mathrm{CC}} \subset \mathbf{P}^{\mathbf{NP}^{\mathrm{CC}}}$.

Chapter 3

Important examples

In this section, we review the properties of some specific examples of matrices and functions. These will be used in the later chapters.

3.1 Equality function

As usual denote by $\mathtt{J}_n$ the $n \times n$ all-one matrix.

Example 3.1 (Identity Matrix, Equality Function)**.** *The $n \times n$ identity matrix $\mathtt{I}_n$, and its complement $\overline{\mathtt{I}}_n \coloneqq \mathtt{J}_n - \mathtt{I}_n$ satisfy the following.*

(i) See [KN97, Example 3.9]:

$$\mathrm{R}_0(\mathtt{I}_n) = \mathrm{R}_0(\overline{\mathtt{I}}_n) = \Theta(\log(n)).$$

(ii) See [KN97, Example 3.9]:

$$\mathrm{R}^1(\mathtt{I}_n) = \Theta(\log(n)), \ \textit{and} \ \mathrm{R}^1(\overline{\mathtt{I}}_n) = O(1),$$

In particular, $\mathrm{R}(\mathtt{I}_n) = O(1)$.

Proof. (i) The upper bounds follow from the trivial protocol and the lower bounds follow from Proposition 2.5 as the covering number $C^1(\mathtt{I}_n) = \Omega(n)$.

(ii) By the same arguments, $\mathrm{R}^1(\mathtt{I}_n) = \Theta(\log n)$.

Next, we bring an one-sided error randomized protocol which computes $\overline{\mathtt{I}}_n$ with $O(1)$ cost. Let x be Alice's input, y be Bob's input and $r \in \{0,1\}^{\log n}$ be the common random string. The protocol is the following:

> Alice computes $a := \sum_i x_i r_i \pmod 2$ and sends a to Bob. Bob, in his turn, computes $b := \sum_i y_i r_i \pmod 2$ and compares b with a. If $a = b$, the protocol outputs 0, otherwise it outputs 1.

The protocol requires only two bits. For the correctness, note that if $x = y$, then $a = b$, hence the protocol outputs the correct answer without an error. If $x \neq y$, then $a = b$ with 1/2 probability, hence on 1-inputs the error probability is 1/2. Repeating this protocol for one more time will reduce the error probability to $\frac{1}{4} < \frac{1}{3}$.

□

3.2 Greater-than function

We consider the *greater-than* matrix, where all the entries on the diagonal and below it are 0, and all the entries above the diagonal are 1.

Example 3.2 (Greater-than)**.** *The $n \times n$ greater-than matrix GT_n, defined as $\mathrm{GT}_n(i,j) = 1$ if and only if $i < j$, and its complement $\overline{\mathrm{GT}}_n := \mathtt{J}_n - \mathrm{GT}_n$ satisfy the following.*

(i) See [KN97, Exercise 3.10]:

$$\mathrm{R}^1(\mathrm{GT}_n) = \Theta(\log(n)), \textit{ and } \mathrm{R}^1(\overline{\mathrm{GT}}_n) = \Theta(\log(n)).$$

In particular,

$$\mathrm{R}_0(\mathrm{GT}_n) = \mathrm{R}_0(\overline{\mathrm{GT}}_n) = \Theta(\log(n)).$$

(ii) See [Vio15, RS15] and [KN97, Exercise 3.18]:

$$\mathrm{R}(\mathrm{GT}_n) = \Theta(\log\log(n)).$$

Proof. (i) The trivial protocol gives the upper bounds, and the lower bounds follow from Proposition 2.5 as the 1-covering number $C^1(\mathrm{GT}_n) = \Omega(n)$.

(ii) $\mathrm{R}(\mathrm{GT}_n) = O(\log^2(\log n))$ can be achieved by doing a binary search. A more careful analysis yields the upper bound of $O(\log\log n)$ suggested [KN97, Exercise 3.18]. The lower bound is proven in [Vio15, RS15] .

□

3.3 Threshold functions

For an integer $k \geq 0$, define the *threshold function* $\mathrm{thr}_k : \{0,1\}^n \to \{0,1\}$ as $\mathrm{thr}_k(x) = 1$ if and only if $\sum_{i=1}^n x_i \geq k$. We will also write $\overline{\mathrm{thr}}_k = 1 - \mathrm{thr}_k$.

Denote the XOR and AND-lifts of thr_k as $\mathrm{Thr}_k^{\oplus}(x,y) = \mathrm{thr}_k(x \oplus y)$ and $\mathrm{Thr}_k^{\wedge}(x,y) = \mathrm{thr}_k(x \wedge y)$, respectively. Recall that $\mathrm{rk}_{\oplus}(f)$ denotes the number of non-zero Fourier coefficients of a function $f : \{0,1\}^n \to \{0,1\}$, which is also equal to the rank of $F^{\oplus}(x,y) \coloneqq f(x \oplus y)$.

Lemma 3.3 (Threshold function in the XOR-model)**.** *For every* $0 \leq k \leq n$*, we have*

(i) $\mathrm{rdt}^{\oplus}(\mathrm{thr}_k) \leq \mathrm{rdt}^{\oplus 1}(\mathrm{thr}_k) = 2^{O(k)}$*. In particular,* $\mathrm{R}(\mathrm{Thr}_k^{\oplus}) = 2^{O(k)}$*.*

(ii) We have $\mathrm{rk}_{\oplus}(\mathrm{thr}_k) = \mathrm{rk}(\mathrm{Thr}_k^{\oplus}) \geq 2^{n/2}$*, and consequently* $\mathrm{dt}^{\oplus}(\mathrm{thr}_k) = \Omega(n)$*.*

Proof. (i) The randomized protocol will first randomly partition $\{1,\ldots,n\}$ into sets $S_1,\ldots,S_k$, where each element $j \in [n]$ is uniformly and independently assigned to one of the k sets. Next, for each $i \in [k]$, pick a subset $T_i \subseteq S_i$ uniformly at random, and query $\oplus_{j\in T_i} x_j$. Output 1 if all the queries are 1, and output 0 otherwise.

If $\mathrm{thr}_k(x) = 0$, then we will always correctly output 0, as in this case there always exists i such that $x|_{S_i}$ is all zeros. On the other hand, if $\mathrm{thr}_k(x) = 1$, with probability at least $\frac{k!}{k^k} \geq e^{-k}$, every S_i will contain at least one 1. Conditioned on the prior event, with probability at least 2^{-k} every query satisfies $\oplus_{j\in T_i} x_j = 1$, in which case the protocol correctly outputs 1. Thus, the probability of error is at most $1-(2e)^{-k}$. Finally, by standard error-reduction, repeating this procedure $2^{O(k)}$ times can reduce the error to at most $1/3$. We conclude that there is a constant $c_k = 2^{O(k)}$ such that $\mathrm{rdt}^{\oplus 1}(\mathrm{thr}_k) = c_k$.

(ii) First note that fixing the values of variables can only decrease the size of the support of the Fourier transform. Now if $k \leq n/2$, then setting $k-1$ of the variables to 1 will result in the function that is 1 everywhere except on $\mathbf{0}$. This restricted function has a full Fourier support, which is of size $2^{n-k+1} \geq 2^{n/2}$. Similarly, if $k \geq n/2$, then setting $n-k$ of the variables to 0 yields a function which is 0 everywhere except on $\mathbf{1}$. Hence this function has a full Fourier support, which is of size $2^k \geq 2^{n/2}$.

Next, Proposition 5.1 from below implies

$$\mathrm{dt}^{\oplus}(\mathrm{thr}_k) \geq \frac{1}{2} \log \mathrm{rk}_{\oplus}(\mathrm{thr}_k) \geq \frac{n}{4}.$$

□

The threshold functions are also important instances for the AND-query model.

Lemma 3.4 (Threshold functions in AND-model [KLMY20, Example 6.3])**.** *For every fixed $0 \leq k \leq n$, we have*

(i) $\mathrm{dt}^{\wedge}(\mathrm{thr}_k) \geq \log \binom{n}{k} \sim n \cdot \mathrm{H}(\frac{k}{n})$, *where* H *is the binary entropy function defined as* $H(x) = -x \log_2 x - (1-x)\log_2(1-x)$.

(ii) $\mathrm{rdt}^{\wedge}(\mathrm{thr}_{n-k}) = \mathrm{rdt}^{\wedge}(\overline{\mathrm{thr}}_{n-k}) \leq \mathrm{rdt}^{\wedge 1}(\overline{\mathrm{thr}}_{n-k}) = 2^{O(k)}$.

In particular, $\mathrm{R}(\mathrm{Thr}^{\wedge}_{n-k}) = 2^{O(k)}$.

Proof. (i) Consider an AND-decision tree T computing thr_k. It suffices to show that T has at least $\binom{n}{k}$ leaves. Let $\binom{[n]}{k}$ denote the set of all elements of Hamming weight exactly k. Note that if the output of a query $\wedge_{i \in S}$ is the same for two elements $x, y \in \{0,1\}^n$, then the query will also return the same value for $x \wedge y$. This shows that the computation in T for two distinct $x, y \in \binom{[n]}{k}$ cannot lead to the same leaf, as then $x \wedge y$ must also lead to the same leaf, but $1 = \mathrm{thr}_k(x) \neq \mathrm{thr}_k(x \wedge y) = 0$.

(ii) Note that $\overline{\mathrm{thr}}_{n-k}(x) = 1$ if and only if $x \in \{0,1\}^n$ contains at least $k+1$ 0's. We partition $[n]$ uniformly at random into $k+1$ sets $S_1, \ldots, S_{k+1}$, and query $\wedge_{j \in S_i} x_j$ for $i \in [k+1]$.

If all of the queries return 0, we output 1, and otherwise we output 0. This protocol is always correct on inputs x with $\overline{\mathrm{thr}}_{n-k}(x) = 0$, and furthermore for inputs with $\overline{\mathrm{thr}}_{n-k}(x) = 1$, the probability of error is at most $1 - \frac{(k+1)!}{(k+1)^{k+1}} \leq 1 - e^{k+1}$. The claim now follows from standard error reduction. □

Finally, we prove a lower bound on the Fourier algebra norm of threshold functions.

Lemma 3.5 (Fourier algebra norm of threshold functions)**.** *For $k \leq n/2$, we have*

$$e^{-(k-1)}\sqrt{\sum_{i=0}^{k-1}\binom{n}{i}} \leq \left\|\overline{\mathrm{thr}}_k\right\|_A \leq \sqrt{\sum_{i=0}^{k-1}\binom{n}{i}}.$$

In particular, by Corollary 4.16, the same bounds hold for $\|\overline{\mathrm{Thr}}_k^{\oplus}\|_{\mathrm{ntr}} = \|\overline{\mathrm{Thr}}_k^{\oplus}\|_{\gamma_2}$.

Proof. Define $p : \{-1,1\}^n \to \mathbb{R}$ as

$$p(y) = \sum_{\substack{S\subseteq[n] \\ |S|\leq k-1}} \prod_{i\in S} y_i,$$

and note that $p(y) = \sum_{x\in\{0,1\}^n} \overline{\mathrm{thr}}_k(x)\chi_{T_y}(x) = 2^n\widehat{\overline{\mathrm{thr}}_k}(T_y)$, where $T_y = \{i : y_i = -1\}$. Hence,

$$\|\overline{\mathrm{thr}}_k\|_A = \frac{1}{2^n}\sum_y |p(y)| = \|p\|_{L^1(\{-1,1\}^n)}.$$

By Parseval

$$\|p\|_{L^2(\{-1,1\}^n)} = \sqrt{\sum_{i=0}^{k-1}\binom{n}{i}},$$

and furthermore, since $\deg(p) \leq k-1$, by generalization of Khintchine's inequality to degree $k-1$ polynomials ([O'D14, Theorem 9.22]), we have

$$e^{-(k-1)}\|p\|_{L^2(\{-1,1\}^n)} \leq \|p\|_{L^1(\{-1,1\}^n)} \leq \|p\|_{L^2(\{-1,1\}^n)}.$$

□

Chapter 4

Main results: General matrices

We start by proving the results that apply to general Boolean matrices. Later, in Chapter 5 and Chapter 6, we study special classes of XOR and AND-matrices.

4.1 Blocky matrices and blocky-rank

As we have discussed earlier, EQ provides a separation between deterministic communication complexity and randomized communication complexity, in both one-sided and two-sided error models. Now suppose that we equip the players, Alice and Bob, with an *equality oracle*. To be more precise, we allow these protocols to have query nodes v, on which the players map their inputs to strings $\alpha_v(x)$ and $\beta_v(y)$, respectively, and the oracle will broadcast the value of $\mathrm{EQ}(\alpha_v(x), \beta_v(y))$ to both players. This will contribute only one bit to the communication cost which is measured in bits. Note that the usual communicated bits can also be simulated by oracle queries. For example, if it is Alice's turn to send a bit $a_v(x)$, then she can use the query $\mathrm{EQ}(a_v(x), 1)$ to transmit this bit to Bob. Hence, in this model, we can assume that all the communication is done through oracle queries.

Obviously, having access to an equality oracle, Alice and Bob can solve EQ deterministically at cost $O(1)$, namely by querying the oracle for $\mathrm{EQ}(x, y)$.

Let $\mathrm{D}^{\mathrm{EQ}}(M)$ denote the smallest cost of a deterministic protocol with equality oracle for the matrix M.

Proposition 4.1. *Let $M : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ be a matrix. Then*

$$\frac{1}{2}\log \operatorname{rk}(\mathcal{Blocky}, M) \leq \mathrm{D}^{\mathrm{EQ}}(M) \leq \operatorname{rk}(\mathcal{Blocky}, M),$$

and

$$\frac{1}{2}\log \|M\|_{\mathcal{Blocky}} \leq \mathrm{D}^{\mathrm{EQ}}(M).$$

Proof. We first prove $\mathrm{D}^{\mathrm{EQ}}(M) \leq \operatorname{rk}(\mathcal{Blocky}, M)$. Let $k = \operatorname{rk}(\mathcal{Blocky}, M)$. We construct an EQ-oracle protocol for f. In advance, Alice and Bob agree on a decomposition $M = \sum_{i=1}^{k} \lambda_i M_i$, where M_i is a blocky matrix and $\lambda_i \in \mathbb{R}$ for $i \in [k]$. Since each blocky matrix M_i corresponds to an EQ query, for an input (x, y) Alice and Bob make k queries to the oracle to determine $M_1(x, y), \ldots, M_k(x, y)$. At this point both Alice and Bob can compute $M(x, y) = \sum_{i=1}^{k} \lambda_i M_i(x, y)$.

For the lower bounds, let $d = \mathrm{D}^{\mathrm{EQ}}(M)$. Consider a leaf ℓ in the EQ-oracle protocol tree computing M and let P_ℓ denote the path of length $k_\ell \leq d$ from the root to ℓ. Note that each non-leaf node v in the tree corresponds to a query to the equality oracle, and each such query corresponds to a blocky matrix B_v. For the matrix M_v, define $B_v^1 = B_v$ and $B_v^0 = \overline{B}_v = \mathrm{J}_{\mathcal{X}\times\mathcal{Y}} - B_v$.

Suppose $P_\ell = v_1, v_2, \ldots, v_{k_\ell}, \ell$, and consider the matrix

$$M_{P_\ell} := B_{v_1}^{\sigma_{v_1}} \circ B_{v_2}^{\sigma_{v_2}} \circ \ldots \circ B_{v_{k_\ell}}^{\sigma_{v_{k_\ell}}},$$

where $\sigma_{v_i} \in \{0,1\}$ and $\sigma_{v_i} = 1$ if and only if the edge (v_{i-1}, v_i) is labeled by 1. Hence, after simplification, M_{P_ℓ} can be written as a sum of at most 2^d summands with ± 1 coefficients, where each summand is a Schur product of at most k_l blocky matrices. Observe that the Schur product of two blocky matrices is a blocky matrix. Thus, M_{P_ℓ} can be written as a sum of at most 2^d blocky matrices with ± 1 coefficients.

Summing over all the leaves that are labeled by 1, we get

$$M = \sum_{\ell \text{ is a 1-leaf}} M_{P_\ell}.$$

As the number of leaves is bounded by 2^d, and each M_{P_ℓ} is a ± 1 linear combination of at most 2^d blocky matrices, it follows that $\mathrm{rk}(\mathcal{Blocky}, M) \leq 2^{2d}$ and $\|M\|_{\mathcal{Blocky}} \leq 2^{2d}$. □

Combining the two inequalities, we have the following useful relation

$$\frac{1}{2} \log \|M\|_{\mathcal{Blocky}} \leq \mathrm{rk}(\mathcal{Blocky}, M). \tag{4.1}$$

The opposite direction turns out to be equivalent to Conjecture III.

Conjecture 4.2. *There exists $\kappa : \mathbb{R}^+ \to \mathbb{R}^+$ such that for a Boolean matrix M,*

$$\mathrm{rk}(\mathcal{Blocky}, M) \leq \kappa(\|M\|_{\mathcal{Blocky}}).$$

Proposition 4.3. *Conjecture 4.2 and Conjecture III are equivalent.*

Proof. Conjecture III $\Longrightarrow$ Conjecture 4.2: Conjecture III implies that there is a function $\tau : \mathbb{R}^+ \to \mathbb{R}^+$ such that M can be written as a sum of $\tau(\|M\|_\mu)$ blocky matrices with ± 1 coefficients. Hence, by Equation (2.6),

$$\mathrm{rk}(\mathcal{Blocky}, M) \leq \tau(4 \cdot \|M\|_{\mathcal{Blocky}}).$$

Conjecture 4.2 $\Longrightarrow$ Conjecture III: By the proof of Proposition 4.1, M can be written as a sum of $2^{2\,\mathrm{D}^{\mathrm{EQ}}(M)}$ blocky matrices with ± 1 coefficients. If Conjecture 4.2 is true, then for some $\kappa : \mathbb{R}^+ \to \mathbb{R}^+$,

$$\mathrm{D}^{\mathrm{EQ}}(M) \leq \mathrm{rk}(\mathcal{Blocky}, M) \leq \kappa(\|M\|_{\mathcal{Blocky}}). \tag{4.2}$$

Now, by the assumption of Conjecture III, $\|M\|_\mu \leq c$ for some constant c. Recall from Equation (2.6) that $\|M\|_{\mathcal{Blocky}} \leq \|M\|_\mu$, so $\|M\|_{\mathcal{Blocky}} \leq c$. Combining this with Equation (4.2), we conclude that M can be written as a sum of $k_c := 2^{2\kappa(c)}$ blocky matrices with ± 1 coefficients. □

4.1.1 Relation of blocky-rank to randomized communication complexity and Conjecture I

Proposition 4.4. *For a function $f : \mathcal{X} \times \mathcal{Y} \to \{0, 1\}$,*

$$\mathrm{R}(f) \leq O(\mathrm{D}^{\mathrm{EQ}}(f) \cdot \log \mathrm{D}^{\mathrm{EQ}}(f)).$$

Proof. Suppose $d := \mathrm{D}^{\mathrm{EQ}}(f)$. An EQ oracle protocol tree of depth d can be used to design a randomized protocol for f: The parties simply simulate the tree, where at each node the equality oracles are simulated (up to some error probability) via an efficient randomized communication protocol for EQ. By a simple union bound, to ensure that the final error is bounded by 1/3, it suffices to use randomized equality protocols with error at most $\frac{1}{3d}$. Recall that by Example 3.1, $\mathrm{R}(\mathrm{EQ}) = O(1)$, and thus $\mathrm{R}_{\frac{1}{2^c}}(\mathrm{EQ}) \leq O(c)$. As a result, $\mathrm{R}_{\frac{1}{3d}}(\mathrm{EQ}) \leq O(\log d)$ and $\mathrm{R}(f) \leq O(d \log d)$. □

It follows from this, and Proposition 4.1 that

$$\mathrm{R}(f) \leq O(\mathrm{rk}(\mathcal{B}locky, f) \cdot \log \mathrm{rk}(\mathcal{B}locky, f)). \tag{4.3}$$

The function $\overline{\mathrm{Thr}_2^{\oplus}}$ from Lemma 3.3 demonstrates that the opposite relation is not true – small randomized communication does not imply having a small $\mathrm{rk}(\mathcal{B}locky, \cdot)$. Indeed, by Lemma 3.3 (i), $\mathrm{R}(\overline{\mathrm{Thr}_2^{\oplus}}) = \mathrm{R}(\mathrm{Thr}_2^{\oplus}) = O(1)$. On the other hand, since the γ_2 norm of every blocky matrix is at most 1, by Equation (4.1), we have

$$\mathrm{rk}(\mathcal{B}locky, \overline{\mathrm{Thr}_2^{\oplus}}) \geq \frac{1}{2} \log \|\overline{\mathrm{Thr}_2^{\oplus}}\|_{\mathcal{B}locky} \geq \frac{1}{2} \log \|\overline{\mathrm{Thr}_2^{\oplus}}\|_{\gamma_2},$$

and by Lemma 3.5, we have

$$\log \|\overline{\mathrm{Thr}_2^{\oplus}}\|_{\gamma_2} \geq \Omega(\log n).$$

Remark. By the above discussion, $\overline{\mathrm{Thr}_2^{\oplus}}$ witnesses a gap of $O(1)$ vs. $\Omega(\log(n))$ between randomized communication complexity and deterministic communication complexity with access to equality oracle. The difference between these two parameters had also been studied in [CLV19], where a function with $\mathrm{R}(f) = O(\log(\log n))$ and $\mathrm{D}^{\mathrm{EQ}}(f) = \Omega(\log(n))$ is exhibited. However, the separation of [CLV19] was not ruling out a dimension-free relation between these parameters.

As Equation (4.3) shows, randomized communication complexity can be upper-bounded by a function of blocky-rank, and thus it is natural to wonder whether a relaxation of Conjecture I holds for matrices with bounded blocky-rank, or equivalently $\mathrm{D}^{\mathrm{EQ}}(\cdot) = O(1)$. It is not hard to see that this is indeed true.

Lemma 4.5. *If an $n \times n$ matrix M satisfies $\mathrm{rk}(\mathcal{Blocky}, M) \leq c$, then M has a monochromatic rectangle of size $\delta_c n \times \delta_c n$, where $\delta_c > 0$ only depends on c.*

Proof. We prove by induction on c that the statement is true with $\delta_c \geq 3^{-c}$. As the base case we first show that every $n \times n$ blocky matrix has an $n/3 \times n/3$ monochromatic rectangle. Suppose B is a blocky matrix with blocks $X_1 \times Y_1, \ldots, X_t \times Y_t$. We assume without loss of generality that $|\cup_i X_i| \geq 2n/3$, as otherwise $([n] \setminus \cup_i X_i) \times [n]$ contains an $n/3 \times n/3$ all-zero rectangle. Moreover, note that if for some $i \in [t]$, $|X_i| \geq n/3$, then one of $X_i \times Y_i$ or $X_i \times [n] \setminus Y_i$ contains an $n/3 \times n/3$ monochromatic rectangle. Now, suppose that for all i, $|X_i| < n/3$. This implies that there is k such that $\sum_{i=1}^{k} |X_i| \in (n/3, 2n/3)$. Note that both $(\cup_{i \leq k} X_i) \times ([n] \setminus \cup_{i \leq k} Y_i)$ and $([n] \setminus \cup_{i \leq k} X_i) \times (\cup_{i \leq k} Y_i)$ are monochromatic rectangles, and furthermore one of them contains an $n/3 \times n/3$ monochromatic rectangle.

Now suppose that M is an $n \times n$ matrix such that $M = \sum_{i=1}^{m} \lambda_i B_i$, where B_i are blocky matrices. By the base case, B_m has an $n/3 \times n/3$ monochromatic rectangle $X \times Y$. Then

$$M' \coloneqq (M - \lambda_m B_m)|_{X \times Y} = \sum_{i=1}^{m-1} \lambda_i B_i|_{X \times Y},$$

which shows $\mathrm{rk}(\mathcal{Blocky}, M') \leq c - 1$. Consequently, M' has an $\frac{|X|}{3^{c-1}} \times \frac{|Y|}{3^{c-1}}$ monochromatic rectangle, which translates to an $\frac{n}{3^c} \times \frac{n}{3^c}$ monochromatic rectangle in M. □

Lemma 4.5 combined with the lower bound from Proposition 4.1 implies that a weaker version of Conjecture I holds where instead of assuming bounded randomized communication complexity, one makes the stronger assumption that $\mathrm{D}^{\mathrm{EQ}}(\cdot) = O(1)$.

4.2 Zero-error complexity and approximate-rank are qualitatively equivalent to rank

In this section, we prove that both approximate-rank, and zero-error randomized communication complexity are qualitatively equivalent to the rank, and deterministic communicating complexity.

It is known that, allowing a loss of $O(\log\log(n))$, the gap between the zero-error randomized communication complexity, and the deterministic communication complexity of an $n \times n$ matrix M can be at most quadratic [KN97, Exercise 3.15]:

$$\Omega(\sqrt{\mathrm{D}(M)} - \log\log(n)) \leq \mathrm{R}_0(M) \leq \mathrm{D}(M).$$

The above bound does not provide a dimension-free equivalence between $\mathrm{D}(M)$ and $\mathrm{R}_0(M)$ due to the $O(\log\log(n))$ term which is from applying Newman's theorem to convert zero-error private randomness to zero-error public randomness. To obtain a dimension-free equivalence, we use a different method.

Our approach is to find copies of submatrices that have large zero-error randomized communication complexity in every high-rank Boolean matrix. The following key lemma states that if the rank of a Boolean matrix is sufficiently large, then it must contain, as a submatrix, a large copy of at least one of the four matrices: the identity matrix $\mathtt{I}_k$, its complement $\overline{\mathtt{I}}_k$, greater-than function GT_k, or its complement $\overline{\mathrm{GT}}_k$.

Lemma 4.6 (Key lemma for zero-error and approximate-rank)**.** *Let M be a Boolean matrix of rank r, and let $k = \log_5(r)/4$. Then M contains a copy of at least one of $\mathtt{I}_k$, $\overline{\mathtt{I}}_k$, GT_k, or $\overline{\mathrm{GT}}_k$ as a submatrix.*

Proof. The proof is similar to the proof of the existence of Ramsey numbers. Let $R(k_1, k_2, k_3, k_4)$ be the smallest r such that every Boolean matrix of rank r, contains a copy of at least one of $\mathtt{I}_{k_1}$, $\overline{\mathtt{I}}_{k_2}$, GT_{k_3}, or $\overline{\mathrm{GT}}_{k_4}$. We will show by induction that

$$R(k_1, k_2, k_3, k_4) \leq 5^{k_1+k_2+k_3+k_4}. \tag{4.4}$$

The base cases are when $k_i = 1$ for some $i \in \{1, \dots, 4\}$, in which case $R(k_1, k_2, k_3, k_4) \leq 2$, as any matrix of rank 2 must contain both 0 and 1 entries, and thus must contain, as a submatrix, a copy of each of $\mathtt{I}_1, \overline{\mathtt{I}}_1, \mathrm{GT}_1, \overline{\mathrm{GT}}_1$.

To prove the induction step, assume $k_i \geq 2$ for all $i \in [4]$, and consider a Boolean matrix $M = [a_{ij}]_{m\times n}$ of rank at least $5^{k_1+k_2+k_3+k_4}$. Since $\mathrm{rk}(M) \geq 2$, then M contains both 0's and

1's so we may assume without loss of generality that the n-th column contains both 0's and 1's. This partitions the rows of the matrix into two non-empty sets:

$$R_0 = \{i \in [m] : a_{in} = 0\} \text{ and } R_1 = \{i \in [m] : a_{in} = 1\}.$$

Let $a \in \{0, 1\}$ be chosen such that $R_a \times [n]$ corresponds to the submatrix with the larger rank, that is

$$\mathrm{rk}(M|_{R_a \times [n]}) \geq \mathrm{rk}(M)/2,$$

where we used the subadditivity of rank. By permuting the rows if necessary, we can assume that $m \notin R_a$, or equivalently $a_{mn} \neq a$. Define

$$C_0 = \{j \in [n] : a_{mj} = 0\} \text{ and } C_1 = \{j \in [n] : a_{mj} = 1\}.$$

Let M_{00} be the submatrix of M on $(R_0 \cap [m-1]) \times (C_0 \cap [n-1])$, and define M_{01}, M_{10}, M_{11} similarly (see Figure 4.1).

For a matrix N, let $m_{\mathtt{I}}(N)$ denote the largest k such that N contains a copy of $\mathtt{I}_k$. Define $m_{\overline{\mathtt{I}}}(N)$, $m_{\mathrm{GT}}(N)$, and $m_{\overline{\mathrm{GT}}}(N)$ similarly.

If $a_{mn} = 1$, then

$$m_{\mathtt{I}}(M) \geq m_{\mathtt{I}}(M_{00}) + 1, \qquad \text{and} \qquad m_{\overline{\mathrm{GT}}}(M) \geq m_{\overline{\mathrm{GT}}}(M_{01}) + 1,$$

since one can use the last row and the last column to extend those submatrices in M_{00} and M_{01} to larger ones in M. Note also that in this case, since $a = 0$,

$$\mathrm{rk}(M_{00}) + \mathrm{rk}(M_{01}) \geq \mathrm{rk}(M|_{R_0 \times [n]}) \geq \mathrm{rk}(M)/2,$$

which implies that either

$$\mathrm{rk}(M_{00}) \geq 5^{k_1+k_2+k_3+k_4-1} \geq R(k_1 - 1, k_2, k_3, k_4),$$

or

$$\mathrm{rk}(M_{01}) \geq 5^{k_1+k_2+k_3+k_4-1} \geq R(k_1, k_2, k_3, k_4 - 1).$$

In both cases, the induction hypothesis yields the desired bound Equation (4.4).

Similarly if $a_{mn} = 0$, then

$$m_{\overline{\mathtt{I}}}(M) \geq m_{\overline{\mathtt{I}}}(M_{11}) + 1, \qquad \text{and} \qquad m_{\mathrm{GT}}(M) \geq m_{\mathrm{GT}}(M_{10}) + 1,$$

and in this case, since $a = 1$, we obtain

$$\mathrm{rk}(M_{10}) + \mathrm{rk}(M_{11}) + 1 \geq \mathrm{rk}(M|_{R_1 \times [n]}) \geq \mathrm{rk}(M)/2,$$

which implies

$$\mathrm{rk}(M_{10}) \geq 5^{k_1+k_2+k_3+k_4-1} \geq R(k_1, k_2, k_3 - 1, k_4),$$

or

$$\mathrm{rk}(M_{11}) \geq 5^{k_1+k_2+k_3+k_4-1} \geq R(k_1, k_2 - 1, k_3, k_4).$$

Again in both cases, the induction hypothesis implies Equation (4.4) as desired. □

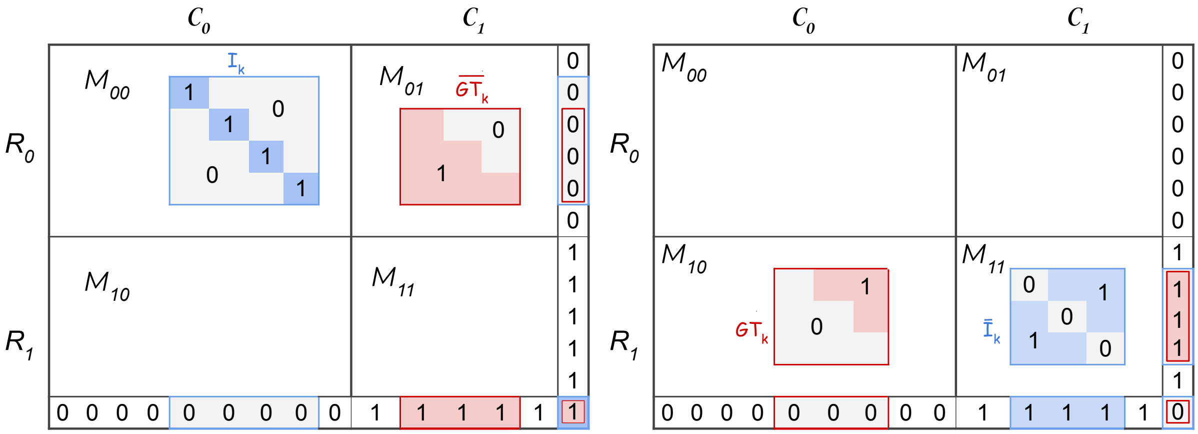


Figure 4.1: The matrix M with the row partitions R_0 and R_1, the column partitions C_0 and C_1, and the respective submatrices M_{00}, M_{01}, M_{10} and M_{11}. When $a_{mn} = 1$, as shown in the left figure, a copy of $\mathtt{I}_k$ in M_{00} can be extended to $\mathtt{I}_{k+1}$, and a copy of $\overline{\mathrm{GT}}_k$ in M_{01} to $\overline{\mathrm{GT}}_{k+1}$. When $a_{mn} = 0$, as in the right figure, a copy of $\overline{\mathtt{I}}_k$ in M_{11} can be extended to $\overline{\mathtt{I}}_{k+1}$, and a copy of GT_k in M_{10} to GT_{k+1}.

Lemma 4.6 shows that zero-error randomized communication complexity and rank are all qualitatively equivalent.

Theorem 4.7 (Equivalence between zero-error and rank)**.** *There exist a constant $c > 0$, such that for every Boolean matrix M, we have*

$$c \log\log \mathrm{rk}(M) \leq \mathrm{R}_0(M) \leq \mathrm{rk}(M), \tag{4.5}$$

Proof. The upper bound in (4.5) follows from $\mathrm{R}_0(M) \leq \mathrm{D}(M)$. It remains to prove the lower bound in (4.5). By Lemma 4.6, we are guaranteed to find a copy of $\mathtt{I}_k$, $\overline{\mathtt{I}}_k$, GT_k, or $\overline{\mathrm{GT}}_k$ as a submatrix in M, where $k = \frac{1}{4}\log_5 \mathrm{rk}(M)$. By Example 3.1 and Example 3.2, all the four matrices $\mathtt{I}_k$, $\overline{\mathtt{I}}_k$, GT_k, $\overline{\mathrm{GT}}_k$ have zero-error randomized communication complexity $\Omega(\log k)$, which yields the lower bound of (4.5).

□

Remark. The lower bound in Equation (4.6) is sharp for identity matrix $\mathtt{I}_n$, as $\mathrm{rk}(\mathtt{I}_n) = n$, but $\mathrm{rk}_\epsilon(\mathtt{I}_n) \geq \Omega\left(\frac{\log(n)}{\epsilon^2 \log(1/\epsilon)}\right)$ for $\frac{1}{2\sqrt{n}} \leq \epsilon \leq \frac{1}{4}$ (see [Alo09]).

Remark. The upper bound of Equation (4.5) follows from $\mathrm{D}(M) \leq \mathrm{rk}(M)$, however Lovett [Lov16] proved a better upper bound for deterministic communication complexity in terms of rank: $\mathrm{D}(M) \leq O(\sqrt{\mathrm{rk}(M)} \log \mathrm{rk}(M))$. Although, quantitatively this is a huge improvement from the previous known upper bound of $O(\mathrm{rk}(M))$, from our perspective Lovett's upper bound does not change the qualitative relation between $\mathrm{D}(M)$ and $\mathrm{rk}(M)$.

Theorem 4.8 ([GS19])**.** *For every $\epsilon < 1/2$, there exists a constant $c_\epsilon > 0$ such that for every Boolean matrix M, we have*

$$c_\epsilon \log_2 \mathrm{rk}(M) \leq \mathrm{rk}_\epsilon(M) \leq \mathrm{rk}(M). \tag{4.6}$$

Proof. The upper bound is trivial, so we sketch their proof of the lower bound here. Let A be the matrix ϵ-approximating M. It will be easier to work with sign matrices, so let $M' = \mathtt{J} - 2M$ and $A' = \frac{1}{1-2\epsilon}(\mathtt{J} - 2A)$ be the sign versions of M and A, respectively. Then for $\alpha := \frac{2}{1-2\epsilon}$, A' α-approximates M', where α-approximation for sign matrices is equivalently defined as $1 \leq M'(x,y)A'(x,y) \leq \alpha$.

Let $r = \mathrm{rk}_\alpha(M')$ and note that it is sufficient to prove that the number of distinct rows (or columns) in M' is at most $2^{c_\alpha r}$ for some $c_\alpha > 0$. Let $v_1 \ldots v_k$ be the rows in A' corresponding to the maximal set of pairwise distinct set of rows in M'. For each pair of rows v_{i_1} and v_{i_2}, where $i_1 \neq i_2$, there exists a column $j \in [n]$ such that $|v_{i_1 j} - v_{i_2 j}| \geq 2$.

Let U be the span of the rows of A' and consider the space $V = U \cap [-\alpha, \alpha]^n$. Note that $v_i \in V$ for all $i \in [k]$. Then, for a vector v and $\lambda > 0$ denote $v + \lambda V = \{v + \lambda u \mid u \in V\}$. Fix $\lambda = \frac{1}{1+\alpha}$, and observe that for each $i \in [k]$, the sets $v_i + \lambda V$ are pairwise disjoint. Hence,

$$k \cdot \text{Volume}\left(\lambda V\right) = \sum_{i=1}^{k} \text{Volume}\left(v_i + \lambda V\right) \leq \text{Volume}\left((1+\lambda)V\right),$$

where the last inequality follows from $v_i + \lambda V \subseteq (1+\lambda)V$ for all $i \in [k]$ and the sets $v_i + \lambda V$ being pairwise disjoint. It follows

$$k \leq \frac{\text{Volume}\left((1+\lambda)V\right)}{\text{Volume}\left(\lambda V\right)} = \frac{(1+\lambda)^r \cdot \text{Volume}(V)}{\lambda^r \cdot \text{Volume}(V)} = (\alpha+2)^r.$$

We deduce that $\mathrm{rk}(M') \leq 2^{c_\alpha r}$, where $c_\alpha = \log_2(\alpha + 2)$. □

Corollary 4.9 (Equivalence between zero-error, rank, approximate rank, and deterministic)**.** *There exist a constant $c > 0$, such that for every Boolean matrix M, we have*

$$c \log\log \mathrm{D}(M) \leq c \log\log \mathrm{rk}(M) \leq \mathrm{R}_0(M) \leq \mathrm{D}(M) \leq \mathrm{rk}(M),$$

and for every $\epsilon < 1/2$, there exists a constant $c_\epsilon > 0$ such that

$$c_\epsilon \log_2 \mathrm{rk}(M) \leq \mathrm{rk}_\epsilon(M) \leq \mathrm{rk}(M).$$

Proof. The corollary follows immediately from Theorems 4.7 and 4.8, and $\mathrm{R}_0(M) \leq \mathrm{D}(M)$. □

4.3 One-sided error complexity

In this section, we consider one-sided error randomized protocols, and study the structure of matrices M that satisfy $\mathrm{R}^1(M) = O(1)$. As in the case of two-sided error randomized communication, the identity matrix (Example 3.1) shows that there is a gap between rank and one-sided error randomized communication complexity. The XOR lift of the threshold function also witnesses such a gap; for a constant k, we have $\mathrm{R}^1(\mathrm{Thr}_k^\oplus) = O(1)$ and

$\mathrm{rk}(\mathrm{Thr}_k^{\oplus}) \geq 2^{\Omega(n)}$ by Lemma 3.3. These examples demonstrate that even for matrices with uniformly bounded one-sided error randomized communication complexity we cannot hope to obtain a full structure through bounded rank. Therefore, similar to the theme of Conjecture I, we focus on finding a highly structured object in such matrices.

Theorem 4.10 (Conjecture I for one-sided error)**.** *For every $c > 0$, there exists a constant $\delta_c > 0$ such that if the* one-sided error *randomized communication complexity* $\mathrm{R}^1(M)$ *of an $n \times n$ Boolean matrix M is bounded by c, then it contains an all-zero or all-one $\delta_c n \times \delta_c n$ submatrix.*

Proof. Let t be a constant not depending on n and c; the value of t will be determined later. Assume $n > 2^{\frac{c}{t}+1}$, as otherwise the claim is trivial with $\delta_c = 2^{-\frac{c}{t}-1}$ for all constant t. Fix a small constant $0 < \varepsilon < 2^{-\frac{2c}{t}-4}$. We will assume $|\mathrm{supp}(M)| < \varepsilon n^2$, as otherwise we can find a large all-one submatrix as follows: Given a one-sided error randomized protocol π_R for M with communication at most c, there is a fixing of the randomness r, so that $S = \{(x, y) \mid \pi_r(x, y) = 1\}$ satisfies $|S| \geq \epsilon n^2/3$, where π_r is a deterministic protocol. As π_R is a one-sided error protocol, we have $S \subseteq \mathrm{supp}(M)$. Since π_r is deterministic, then it provides a partitioning of S into at most 2^c all-one submatrices. As a result, M has an all-one submatrix of size at least $\frac{\varepsilon n^2}{3 \cdot 2^c}$.

Let S be the maximal subset of $\mathrm{supp}(M)$ such that for any distinct pairs $(x_1, y_1), (x_2, y_2) \in S$, $x_1 \neq x_2$ and $y_1 \neq y_2$. Let $r = |S|$, and note that if $r \leq 2^{\frac{c}{t}}$, then from the maximality of S it follows that deleting all the rows and columns involved in S from M will remove all the 1 entries from M. So the resulting submatrix of M will be all-zero and will have size at least $(n - 2^{\frac{c}{t}}) \times (n - 2^{\frac{c}{t}}) \geq \frac{1}{4} \cdot n^2$, where the inequality follows from t being constant in n and c, and from the assumption of $n > 2^{\frac{c}{t}+1}$. Thus, we may assume $r > 2^{\frac{c}{t}}$.

Denote $k = 2^{\frac{c}{t}}$. By Example 3.1, the identity matrix is hard for one-sided randomized communication, more precisely $\mathrm{R}^1(\mathtt{I}_k) > \tau \log k$ for some constant $\tau > 0$. Fixing $t = \tau$, we get $\mathrm{R}^1(\mathtt{I}_k) > c$.

This means that M cannot contain a copy of the $k \times k$ identity matrix as a submatrix. Thus, every $k \times k$ submatrix of M that contains k entries from S must also have at least one 1-entry outside of S – call such entries off-diagonal 1's. Let m be the number of such off-diagonal 1's in M. The number of $k \times k$ submatrices of M that have k entries from S is $\binom{r}{k}$, and each of these submatrices have at least one off-diagonal 1. In this process, each off-diagonal 1 in M is counted in at most $\binom{r-2}{k-2}$ many submatrices. Hence,

$$m \geq \frac{\binom{r}{k}}{\binom{r-2}{k-2}} \geq \frac{r^2}{4k^2}.$$

Now, if $r \geq 2\sqrt{\varepsilon}k \cdot n$, then $m \geq \varepsilon n^2$, hence $|\mathrm{supp}(M)| \geq \varepsilon n^2$, which is a contradiction to our assumption of $|\mathrm{supp}(M)| < \varepsilon n^2$. So, $r < 2\sqrt{\varepsilon}k \cdot n$. In this case, by deleting all the rows and columns of S from M, we obtain an all-zero rectangle of size at least $(n - 2\sqrt{\varepsilon}k \cdot n)^2 = (1 - 2\sqrt{\varepsilon}k)^2 \cdot n^2$. To sum up, by taking $\delta_c = 1 - 2\sqrt{\varepsilon} \cdot 2^{c/t}$, we get that there is an all-zero rectangle of size at least $\delta_c^2 n^2$.

□

4.4 Idempotent Schur multipliers. An infinite version of Conjecture III

Let $\mathcal{X}$ and $\mathcal{Y}$ be two countable sets. Recall that a matrix $M_{\mathcal{X}\times\mathcal{Y}}$ is a Schur multiplier, if $A \mapsto M \circ A$ defines a map $B(\mathcal{H}_1, \mathcal{H}_2) \to B(\mathcal{H}_1, \mathcal{H}_2)$. In Theorem 2.14, we saw that M is a *contractive idempotent* of the algebra of Schur multipliers if and only if $M \in \mathscr{Blocky}$.

Consequently, if a Boolean matrix $M_{\mathcal{X}\times\mathcal{Y}}$ can be written as a linear combination of finitely many contractive idempotent Schur multipliers, then by the triangle inequality it is a Schur multiplier. More precisely, if $M = \sum_{i=1}^{t} \lambda_i M_i$ is Boolean valued and each M_i is contractive, then M is an idempotent Schur multiplier as $M \circ M = M$, and $\|M\|_m \leq \sum_{i=1}^{t} |\lambda_i|$. This leads to the following conjecture.

Conjecture 4.11. *An (infinite) matrix M is an idempotent Schur multiplier if and only if M is Boolean and can be written as a linear combination of finitely many* contractive *idempotent Schur multipliers.*

A simple compactness argument shows that Conjecture 4.11 is equivalent to Conjecture III.

Remark 1. Conjecture III is equivalent to asking whether M is a linear combination of at most k_c blocky matrices (given the assumption of Conjecture III). Indeed, assume that $M = \sum_{i=1}^{k} \lambda_i M_i$ is an $m \times n$ Boolean matrix, and M_i are blocky matrices. Identify M and each M_i with their supports. Note these are subsets of $[m] \times [n]$. For $k' \leq 2^k$, let $S_1, \ldots, S_{k'}$ be the atoms of the σ-algebra generated by M_i's. Since M is measurable with respect to this σ-algebra, we have $M = \cup_{i \in I} S_i$ for some $I \subseteq \{1, \ldots, k'\}$. Note that for $j \in \{1, \ldots, k'\}$, S_j is an intersection of M_i's and complements of M_i's. The intersection of two blocky matrices is a blocky matrix, and the complement of a blocky matrix B is $\mathtt{J} - B$, where $\mathtt{J}$ is the all-one (blocky) matrix. We conclude that each S_j can be written as a ±1-linear combination of at most 2^k blocky matrices, and thus M can be written as a ±1-linear combination of at most 2^{2k} blocky matrices.

Theorem 4.12. *Conjecture 4.11 and Conjecture III are equivalent.*

Proof. By the equivalence of the norms $\|\cdot\|_\mu$ and $\|\cdot\|_m$, Conjecture III can be rephrased as follows:

For every constant c, there exists a constant k_c such that if a finite Boolean matrix M satisfies $\|M\|_m \leq c$, then there exists k_c blocky matrices B_i and signs $\sigma_i \in \{-1, 1\}$ such that

$$M = \sum_{i=1}^{k_c} \sigma_i B_i.$$

Conjecture 4.11 $\Longrightarrow$ Conjecture III: If Conjecture III is not true, then there must exist an infinite sequence of finite Boolean matrices $\{M_i\}_{i \in \mathbb{N}}$ with $\|M_i\|_m \leq k$ for all i, such that M_i cannot be expressed as a ±1-linear combination of at most i *contractive* idempotent Schur multipliers. Then $M = \oplus_{i \in \mathbb{N}} M_i$ would be an idempotent Schur multiplier, but for every $i \in \mathbb{N}$ it cannot be expressed as a ±1-linear combination of i idempotent contractions. Since M is Boolean, it follows from Remark 1 that M cannot be expressed as a linear combination of at most a finite number of idempotent contractions.

Conjecture III $\Longrightarrow$ Conjecture 4.11: Let M be an idempotent Schur multiplier on $B(\ell_2(\mathcal{X}), \ell_2(\mathcal{Y}))$, and consider a nested sequence $X_1 \subseteq X_2 \subseteq X_3 \ldots$ of *finite* subsets of $\mathcal{X}$, and a nested sequence $Y_1 \subseteq Y_2 \subseteq Y_3 \ldots$ of *finite* subsets of $\mathcal{Y}$ such that $\mathcal{X} \times \mathcal{Y} = \bigcup \mathcal{X}_i \times \mathcal{Y}_i$. Let $M_i = \mathbf{1}_{\mathcal{X}_i \times \mathcal{Y}_i} \circ M$, which can be interpreted as a Schur multiplier on $B(\ell_2(X_i), \ell_2(Y_i))$. Since our sequences are nested, for every $i < j$, we have

$$\mathbf{1}_{X_i \times Y_i} \circ M_j = M_i. \tag{4.7}$$

Furthermore, $\|M_i\|_m \leq \|\mathbf{1}_{X_i \times Y_i}\|_m \cdot \|M\|_m \leq \|M\|_m$, and thus by Conjecture III, there is a constant t, depending only on $\|M\|_m$, such that $M_i = \sum_{k=1}^t \sigma_{i,k} N_{i,k}$ for idempotent contractions $N_{i,k}$. Furthermore by (4.7) for every $j > i$,

$$M_i = \sum_{k=1}^{t} \sigma_{j,k} \left(\mathbf{1}_{X_i \times Y_i} \circ N_{j,k} \right).$$

For a fixed i and k, since $N_{i,k}$, and $\mathbf{1}_{X_i \times Y_i} \circ N_{j,k}$ for all j, are supported on the finite set $X_i \times Y_i$, by restricting to a sub-sequence $i_1 < i_2 < i_3 < \ldots$, we can assume without loss of generality that for every $j \geq i$ we have

$$\mathbf{1}_{X_i \times Y_i} \circ N_{j,k} = N_{i,k}.$$

By restricting to further sub-sequences we can assume this is true for all i, and furthermore for every k, there exists a $\sigma_k \in \{-1, 1\}$ such that $\sigma_{j,k} = \sigma_k$ for all j. To summarize: for all k, and $j > i$,

$$\mathbf{1}_{X_i \times Y_i} \circ N_{j,k} = N_{i,k}, \tag{4.8}$$

and moreover $\sigma_{j,k} = \sigma_k$ for all j, k.

For $k \in \{1, \ldots, t\}$, define the matrix $N_k = [N_k(x,y)]_{x \in \mathcal{X}, y \in \mathcal{Y}}$ as

$$N_k(x,y) = N_{i,k}(x,y),$$

where i is any index such that $(x,y) \in X_i \times Y_i$. This is well-defined since $\mathcal{X} \times \mathcal{Y} = \bigcup X_i \times Y_i$, and (4.8).

Note that N_k is an idempotent contractive Schur multiplier, since, for example, it obviously does not contain any 2×2 submatrix with exactly three 1's. Moreover $M = \sum_{k=1}^t \sigma_k N_k$, which finishes the proof. $\square$

4.5 Group lifts

In this section we focus on the matrices of the form $F(x,y) = f(y^{-1}x)$, where $f : G \to \mathbb{C}$, and G is a finite group. We start by showing that for any finite group G, the Fourier algebra norm of f coincides with the normalized trace norm of its lift $F(x,y) = f(y^{-1}x)$.

Proposition 4.13. *Let G be a finite group, and $f : G \to \mathbb{C}$. Let the matrix $F : G \times G \to \mathbb{C}$ be defined as $F(x,y) = f(y^{-1}x)$. We have*

$$\|f\|_A = \|F\|_{\mathrm{ntr}} \coloneqq \frac{1}{|G|}\|F\|_{\mathrm{tr}}.$$

Proof. Note that the Fourier algebra norm is defined through its dual. The proof will rely on the fact that the dual of the trace norm is the operator norm $\|\cdot\|_{L^2(G)\to L^2(G)}$.

Let $h : G \to \mathbb{C}$, and the matrix H be its lift $H(x,y) = h(y^{-1}x)$. Recall that the convolution operator for h is defined as $L_h : \nu \mapsto \nu * h$, where the convolution is defined by Equation (2.8). Thus, for $\nu : G \to \mathbb{C}$,

$$L_h\nu(x) = \frac{1}{|G|}\sum_{y\in G} h(y^{-1}x)\nu(y) = \frac{1}{|G|}\sum_{y\in G} H(x,y)\nu(y) = \frac{1}{|G|}H\nu(x).$$

Hence,

$$\frac{\|L_h\nu\|_{L^2(G)}}{\|\nu\|_{L^2(G)}} = \frac{\|L_h\nu\|_{\ell_2(G)}}{\|\nu\|_{\ell_2(G)}} = \frac{\|H\nu\|_{\ell_2(G)}/|G|}{\|\nu\|_{\ell_2(G)}},$$

which shows

$$\|L_h\|_{L^2(G)\to L^2(G)} = \frac{1}{|G|}\|H\|_{\ell_2(G)\to\ell_2(G)}.$$

Next, recall that for matrices F and H, $\langle F, H\rangle \coloneqq \sum_{i,j} F_{ij}\overline{H_{ij}} = \mathrm{tr}(FH^*)$, where the overline denotes the conjugate of an entry and H^* denotes the conjugate transpose of H. Now note that

$$\langle f, h\rangle_{L^2(G)} = \frac{1}{|G|^2}\langle f, h\rangle_{\ell_2(G)} = \frac{1}{|G|^2}\langle F, H\rangle \le \frac{1}{|G|^2}\|F\|_{\mathrm{tr}}\|H\|_{\ell_2(G)\to\ell_2(G)} = \|F\|_{\mathrm{ntr}}\|L_h\|_{L^2(G)\to L^2(G)},$$

which shows that

$$\|f\|_A = \sup\left\{\langle f, h\rangle \ : \|L_h\|_{L^2(G)\to L^2(G)} \le 1\right\} \le \|F\|_{\mathrm{ntr}}.$$

On the other hand, let $H : G \times G \to \mathbb{C}$ be such that

$$\|H\|_{\ell_2(G)\to\ell_2(G)} = 1 \qquad \text{and} \qquad \|F\|_{\mathrm{tr}} = \langle F, H\rangle,$$

and let $\widetilde{H} : G \times G \to \mathbb{C}$ be the following symmetrization of H:

$$\widetilde{H}(x, y) = \mathbb{E}_{z\sim G}\, H(zx, zy).$$

By convexity

$$\|\widetilde{H}\|_{\ell_2(G)\to\ell_2(G)} \le \|H\|_{\ell_2(G)\to\ell_2(G)} = 1.$$

Define $h : G \to \mathbb{C}$ by $h(x) = \widetilde{H}(x, 1)$, and note that for every y and x, $h(y^{-1}x) = \widetilde{H}(y^{-1}x, 1) = \widetilde{H}(x, y)$. Since $F(zx, zy) = F(x, y) = f(y^{-1}x)$ for all z, we have

$$\begin{aligned}\langle F, H\rangle = \langle F, \widetilde{H}\rangle &= |G|^2\langle f, h\rangle_{L^2(G)}\\ &\le |G|^2\|f\|_A\|L_h\|_{L^2(G)\to L^2(G)}\\ &= |G|\|f\|_A\|\widetilde{H}\|_{\ell_2(G)\to\ell_2(G)}\\ &\le |G|\|f\|_A,\end{aligned}$$

this shows $\|F\|_{\mathrm{ntr}} \le \|f\|_A$ and completes the proof. □

Davidson and Donsig [DD07] by applying a lemma of Mathias [Mat93] showed that $\|M\|_{\mathrm{ntr}} = \|M\|_m$ if the entries of M are invariant under a transitive group action.

Theorem 4.14 ([DD07]). *Let $\mathcal{X}$ be a* finite *set with a* transitive group action *G on $\mathcal{X}$. Suppose that the matrix $M_{\mathcal{X}\times\mathcal{X}}$ belongs to the commutant of the action G, or equivalently $M(x, y) = M(gx, gy)$ for all $g \in G$. Then*

$$\|M\|_{\mathrm{ntr}} = \|M\|_m = \|M\|_{\gamma_2}.$$

Lemma 4.15 ([Mat93, Lemma 2.4]). *Let $M = [m_{ij}]$ be a complex-valued, $n \times n$ square matrix such that the main diagonal entries of both $|M|$ and $|M^*|$ are the same. Then,*

$$\|M\|_m = \|M\|_{\mathrm{ntr}}.$$

Proof. Let the unitary matrix $W = [w_{ij}]$ be such that $M = W|M|$ be the polar decomposition of M, where $|M| = \sqrt{M^*M}$. Recall, since M is a square matrix there always exists such a W yielding the polar decomposition of M. Let the matrix $\overline{W} = [\overline{w}_{ij}]$ be obtained by taking the complex conjugate of each entry of W, and let $W^* = [w^*_{ij}] = (\overline{W})^T$ be the conjugate transpose of W. Let $\vec{1}$ denote the vector with n 1's and e_i denote the vector which is 1 on i-th coordinate and 0 elsewhere.

First we show the lower bound. From the definitions of Schur norm and operator norm

$$\|M\|_m \geq \|M \circ \overline{W}\|_{2\to 2} \geq \frac{\|(M \circ \overline{W}) \cdot \vec{1}\|_2}{\|\vec{1}\|_2} = \frac{\|(M \circ \overline{W}) \cdot \vec{1}\|_2 \cdot \|\vec{1}\|_2}{\|\vec{1}\|_2 \cdot \|\vec{1}\|_2} \geq \frac{1}{n}\langle (M \circ \overline{W}) \cdot \vec{1}, \vec{1}\rangle, \quad (4.9)$$

where the last inequality follows from Cauchy-Scwarz inequality (Lemma 2.2). Next note that the vector $(M \circ \overline{W}) \cdot \vec{1} = \left(\sum_{j=1}^n \overline{w}_{1j} m_{1j}, \ldots, \sum_{j=1}^n \overline{w}_{nj} m_{nj}\right)^T$. It follows,

$$\langle (M \circ \overline{W}) \cdot \vec{1}, \vec{1}\rangle = \sum_{i=1}^n \sum_{j=1}^n \overline{w}_{ij} m_{ij} = \sum_{j=1}^n \sum_{i=1}^n w^*_{ji} m_{ij} = \sum_{j=1}^n (W^*M)_{jj} = \operatorname{Tr}(W^*M) = \operatorname{Tr}(|M|), \quad (4.10)$$

where the last equality is due to W being unitary. Finally, combining Equations 4.9 and 4.10 yields $\|M\|_m \geq \frac{1}{n}\operatorname{Tr}(|M|) = \|M\|_{\text{ntr}}$.

For the upper bound, we again take the polar decomposition of $M = W|M|$. Observe that M^*M and M^*M are Hermitian matrices, it follows $(M^*M)^{1/2} = |M|$ and $(MM^*)^{1/2} = |M^*|$ are also Hermitian matrices. Define the vectors $x_i = |M|^{1/2} e_i$ and $y_j = |M|^{1/2} W^* e_j$ for $i, j \in [n]$ so that $\langle x_i, y_j\rangle = M_{ij}$. Indeed,

$$\begin{aligned}
\langle x_i, y_j\rangle &= \langle |M|^{1/2} e_i, |M|^{1/2} W^* e_j\rangle \\
&= \langle \left(|M|^{1/2} W^*\right)^* |M|^{1/2} e_i, e_j\rangle \\
&= \langle W \left(|M|^{1/2}\right)^* |M|^{1/2} e_i, e_j\rangle \\
&= \langle W|M| e_i, e_j\rangle \\
&= \langle M e_i, e_j\rangle = M_{ij},
\end{aligned}$$

where $\left(|M|^{1/2}\right)^* |M|^{1/2} = |M|^{1/2}$ as $|M|^{1/2}$ is Hermitian, which follows from $|M|$ being Hermitian. Next,

$$\|x_i\|^2 = \langle x_i, x_i\rangle = \langle |M|^{1/2} e_i, |M|^{1/2} e_i\rangle = \langle \left(|M|^{1/2}\right)^* |M|^{1/2} e_i, e_i\rangle = \langle |M| e_i, e_i\rangle = |M|_{ii},$$

where $|M|^{1/2}$ being Hermitian follows from $|M|$ being Hermitian. Similarly,

$$\begin{aligned}\|y_i\|^2 &= \langle |M|^{1/2}W^*e_i, |M|^{1/2}W^*e_i\rangle \\ &= \langle W^*|M^*|^{1/2}e_i, W^*|M^*|^{1/2}e_i\rangle \\ &= \langle \left(W^*|M^*|^{1/2}\right)^* W^*|M^*|^{1/2}e_i, e_i\rangle \\ &= \langle \left(|M^*|^{1/2}\right)^* WW^*|M^*|^{1/2}e_i, e_i\rangle \\ &= \langle \left(|M^*|^{1/2}\right)^* |M^*|^{1/2}e_i, e_i\rangle \\ &= \langle |M^*|e_i, e_i\rangle = |M^*|_{ii},\end{aligned}$$

where $|M|^{1/2}W^* = W^*|M^*|^{1/2}$ since $|M|^{1/2}$ and $|M^*|^{1/2}$ are unitarily equivalent, namely $|M|^{1/2} = W^*|M^*|^{1/2}W$, and $|M^*|^{1/2}$ is Hermitian as $|M^*|$ is Hermitian. By Proposition 2.12,

$$\|M\|_m \leq \max_i \|x_i\| \cdot \max_j \|y_j\| = \sqrt{\max_i |M|_{ii}} \cdot \sqrt{\max_j |M^*|_{jj}}.$$

Since $|M|$ and $|M^*|$ are constant on the main diagonal, $\max_i |M|_{ii} = \frac{1}{n}\operatorname{Tr}(|M|)$ and $\max_j |M^*|_{jj} = \frac{1}{n}\operatorname{Tr}(|M^*|)$.

$|M|$ and $|M^*|$ are unitarily equivalent; there exists a unitary matrix U such that $|M^*| = U^*|M|U$. Then, $\operatorname{Tr}(|M^*|) = \operatorname{Tr}(U^*|M|U) = \operatorname{Tr}(U^*(U|M|)) = \operatorname{Tr}(|M|)$, where we used the fact that $\operatorname{Tr}(AB) = \operatorname{Tr}(BA)$ for any matrix A and B.

Combining up,

$$\|M\|_m \leq \sqrt{\frac{1}{n}\operatorname{Tr}(|M|)} \cdot \sqrt{\frac{1}{n}\operatorname{Tr}(|M^*|)} = \frac{1}{n}\operatorname{Tr}(|M|) = \|M\|_{\text{ntr}}.$$

□

Proof of Theorem 4.14. Observe that if a matrix M satisfies the theorem's condition then all the entries on the main diagonal of M are equal. To satisfy the condition of Lemma 4.15 $|M|$ and $|M^*|$ also must be constant on the diagonal. Indeed, since $|M|$ and $|M^*|$ belong to the C^*-algebra generated by M, then both $|M|$ and $|M^*|$ are in the commutant of the action G, hence they are constant on the diagonal. □

Combining Proposition 4.13 and Theorem 4.14, we obtain the following corollary.

Corollary 4.16. *Let G be a finite group, $f : G \to \mathbb{C}$, and $F : G \times G \to \mathbb{C}$ be its lift defined as $F(x, y) = f(y^{-1}x)$. We have*

$$\|F\|_m = \|F\|_{\gamma_2} = \|F\|_{\mathrm{ntr}} = \|f\|_A.$$

This corollary combined with the non-Abelian version of Cohen's idempotent theorem settles Conjecture II and Conjecture III for matrices of the form $F(x, y) = f(y^{-1}x)$.

Theorem 4.17. *Conjecture II and Conjecture III are true for for the class of functions $F : G \times G \to \{0, 1\}$ of the form $F(x, y) = f(y^{-1}x)$, where G is a finite group, and $f : G \to \{0, 1\}$.*

Proof. By Corollary 4.16,

$$\|F\|_m = \|F\|_{\gamma_2} = \|F\|_{\mathrm{ntr}} = \|f\|_A.$$

Suppose that $\|f\|_A < c$. By the general version of Cohen's idempotent theorem [San11, Theorem 1.2], there is some constant $k = k_c$, subgroups $H_1, \dots, H_k \subseteq G$, elements $a_1, \dots, a_k \in G$, and signs $\sigma_1, \dots, \sigma_k \in \{-1, 1\}$ such that

$$f = \sum_{i=1}^{k} \sigma_i \mathbf{1}_{H_i a_i}.$$

Then

$$F(x, y) = \sum_{i=1}^{k} \sigma_i \times \left(\sum_{b \in H_i \backslash G} \mathbf{1}_{Hb}(x) \mathbf{1}_{a_i^{-1} Hb}(y) \right),$$

and note that each $B_i(x, y) \coloneqq \sum_{b \in H_i \backslash G} \mathbf{1}_{bHa_i}(x) \mathbf{1}_{bH}(y)$ is a blocky matrix as desired. □

4.6 A weaker version of Conjecture IV

In this section, we prove a relaxation of Conjecture IV. We will show that for Boolean functions having a *small approximate Fourier rank* there exists an affine subspace (coset) of $\mathbb{Z}_2^n$ of small codimension on which the function is constant.

Proposition 4.18. *Let $f : \mathbb{Z}_2^n \to \{0, 1\}$ be a Boolean function and let $g : \mathbb{Z}_2^n \to \mathbb{R}$ be such that $\|f - g\|_\infty \leq \frac{1}{3}$, and $\mathrm{rk}_\oplus(g) \leq c$. Then there exists an affine subspace $V \subseteq \mathbb{Z}_2^n$*

of codimension $\delta_c > 0$ such that f is constant on V, where $\delta_c > 0$ is a constant that only depends on c.

Before proving this, let us introduce some notations and a simple claim, which implies the proposition.

For any $\alpha \in \{0,1\}^n$ and $\alpha \neq 0$, the set $A_\alpha^b := \{x : \chi_\alpha(x) = b\}$ for $b \in \{0,1\}$ is an (affine) subspace of $\mathbb{Z}_2^n$ of codimension 1. For a Boolean function $f : \mathbb{Z}_2^n \to \mathbb{R}$ denote by $f|_{A_\alpha^b}$ the restriction of f to a (affine) subspace A_α^b. Given $\alpha \in \{0,1\}^n$, f can be written as

$$f(x) = \sum_{\beta \in \mathbb{Z}_2^n / \langle \alpha \rangle} \left(\hat{f}(\beta) + \hat{f}(\alpha+\beta)\chi_\alpha(x) \right) \chi_\beta(x),$$

where $\mathbb{Z}_2^n/\langle\alpha\rangle$ denotes the cosets of the group $\langle\alpha\rangle = \{0, \alpha\}$. From this representation it follows that under a restriction to A_α^b, the Fourier coefficients $\hat{f}(\beta)$ and $\hat{f}(\alpha+\beta)$ for every β collapse into one Fourier coefficient having absolute value $|\hat{f}(\beta) + (-1)^b \hat{f}(\alpha+\beta)|$. This in particular implies that Fourier sparsity of f does not increase when f is restricted to a subspace.

Claim 4.19. *For a function $f : \mathbb{Z}_2^n \to \mathbb{R}$ with $\mathrm{rk}_\oplus(f) \leq c$ there exists an affine subspace $V \subseteq \mathbb{Z}_2^n$ of codimension $\delta_c > 0$, and f is constant on V.*

Proof. Note that if $\hat{f}(\alpha) \neq 0$ for some $\alpha \neq 0$, then applying the restriction $\chi_\alpha = b$ for any $b \in \{0,1\}$ kills the monomial χ_α in the Fourier expansion of f, so the Fourier rank of f decreases by at least 1. Thus, at most $\mathrm{rk}_\oplus(f)$ such restrictions taken from Fourier expansion of f will make f constant.

□

Proof of Proposition 4.18. Let $\mathrm{rk}_\oplus(g) \leq c$. By Claim 4.19, there exists an affine subspace $V \subseteq \mathbb{Z}_2^n$ of codimension $\delta_c > 0$ such that g is constant on V. Next, note that knowing $g(x)$ for any $x \in \mathbb{Z}_2^n$, one can uniquely recover the value of $f(x)$ by a rounding argument. This in particular implies that if the restricted function $g|_V$ is constant for some subspace $V \subseteq \mathbb{Z}_2^n$, then f's restriction on V is also constant. □

It is easy to see that $\|f\|_A \leq \mathrm{rk}_{\oplus}(f)$ for Boolean f. Similarly, $\|f\|_{A,\epsilon} \leq (1+\epsilon) \cdot \mathrm{rk}_{\oplus,\epsilon}(f)$. Hence, indeed, Proposition 4.18 is a relaxation of Conjecture IV. Interestingly, the following relation between approximate Fourier rank and approximate algebra norm holds.

Lemma 4.20 ([Zha14])**.** *For any $f : \{0,1\}^n \to \mathbb{R}$ and $\delta > \epsilon \geq 0$,*

$$\mathrm{rk}_{\oplus,\delta}(f) \leq O\Big(\|f\|_{A,\epsilon} \cdot n/(\delta-\epsilon)^2\Big).$$

Note that Proposition 4.18 would have implied Conjecture IV if it was possible to get a better upper bound in Lemma 4.20 without the dependency on n. However, the lemma is tight for AND function - it has $O(1)$ approximate algebra norm and $\theta(n)$ approximate Fourier rank.

In relation to log-rank conjecture for XOR functions. The log-rank conjecture has been extensively studied for XOR functions, however it remains open for this subclass of functions. Due to the special property of XOR functions – that is the Fourier rank of a Boolean function is equal to the rank of its XOR-lift matrix – the log-rank conjecture has an interesting equivalent formulation for XOR functions:

Conjecture 4.21 (folklore)**.** *There is an absolute constant C such that for every Boolean function $f : \mathbb{Z}_2^n \to \{0,1\}$ and its XOR-lift $F_{\oplus} : (x,y) \mapsto f(x \oplus y)$ we have*

$$\mathrm{D}(F_{\oplus}) \leq \log^C (\mathrm{rk}_{\oplus}(f)).$$

Given this, the combined results of [TWXZ13] and [HHL18] showed that the log-rank conjecture for XOR functions in fact has even simpler equivalent formulation in Boolean function analysis:

Conjecture 4.22 ([TWXZ13, HHL18])**.** *Let $f : \mathbb{Z}_2^n \to \{0,1\}$ be a Boolean function. There exists an affine subspace $V \in \mathbb{Z}_2^n$ on which f is constant and V is of codimension $\log^C(\mathrm{rk}_{\oplus}(f))$ for some absolute constant $C > 0$.*

Note that this conjecture looks similar to Proposition 4.18. Indeed, the following easy claim shows that Proposition 4.18 is a relaxation of Conjecture 4.22.

Claim 4.23. *For every Boolean function $f : \mathbb{Z}_2^n \to \{0,1\}$ and for every $\epsilon < 1/2$, there exists a constant $c_\epsilon > 0$ such that*

$$c_\epsilon \log(\mathrm{rk}_\oplus(f)) \leq \mathrm{rk}_{\oplus,\epsilon}(f).$$

Proof. Let $h : \mathbb{Z}_2^n \to \mathbb{R}$ be such that $\|f - h\|_\infty \leq \epsilon$ and $\mathrm{rk}_\oplus(h) = \mathrm{rk}_{\oplus,\epsilon}(f)$. Consider the XOR-lifts of f and h, defined as $F_\oplus(x, y) \mapsto f(x \oplus y)$ and $H_\oplus(x, y) \mapsto h(x \oplus y)$, respectively. Note that $\|F_\oplus - H_\oplus\|_\infty \leq \epsilon$, hence $\mathrm{rk}_\epsilon(F_\oplus) \leq \mathrm{rk}(H_\oplus)$. Combining this with the lower bound on approximate rank from Equation (4.6), we deduce that there exists a constant $c_\epsilon > 0$ such that

$$c_\epsilon \log(\mathrm{rk}_\oplus(f)) = c_\epsilon \log(\mathrm{rk}(F_\oplus)) \leq \mathrm{rk}_\epsilon(F_\oplus) \leq \mathrm{rk}(H_\oplus) = \mathrm{rk}_\oplus(h) = \mathrm{rk}_{\oplus,\epsilon}(f).$$

□

It is natural to ask whether the opposite direction of this inequality also holds as the affirmative answer, in combination with Proposition 4.18, will imply Conjecture 4.22, thus also the log-rank conjecture for XOR functions.

Question 1. *Is there an absolute constant $C > 0$ such that for every $\epsilon < 1/2$ and for every Boolean function $f : \mathbb{Z}_2^n \to \{0,1\}$, $\mathrm{rk}_{\oplus,\epsilon}(f) \leq \log^C(\mathrm{rk}_\oplus(f))$?*

After the initial submission of the thesis, Arkadev Chattopadhyay pointed out an example which provides negative answer to this question. We include the example and his proof below.

Consider the inner product function $\mathrm{IP}_{2n} : \{0,1\}^{2n} \to \{0,1\}$ defined by

$$\mathrm{IP}_{2n}(x_1, \ldots, x_n, y_1, \ldots, y_n) = x_1 y_1 + x_2 y_2 + \ldots + x_n y_n \mod 2.$$

A. Chattopadhyay shows that $\mathrm{rk}_\oplus(f) \geq \mathrm{rk}_{\oplus,\epsilon}(\mathrm{IP}_{2n}) = 2^{\Omega(n)}$, thus answering Question 1 negatively.

Claim 4.24 (A. Chattopadhyay). $\mathrm{rk}_{\oplus,\epsilon}(\mathrm{IP}_{2n}) = 2^{\Omega(n)}$.

Proof. Let $g : \{0,1\}^{2n} \to \mathbb{R}$ be such that $\| \mathrm{IP}_{2n} - g\|_\infty \leq \epsilon$ and $\mathrm{rk}_\oplus(g) = \mathrm{rk}_{\oplus,\epsilon}(\mathrm{IP}_{2n})$.

$$\begin{aligned}
\langle \mathrm{IP}_{2n}, g \rangle &= \mathbb{E}_x[\mathrm{IP}_{2n}(x) g(x)] \\
&= \mathbb{E}_x\left[\mathrm{IP}_{2n}(x) \left(\sum_{S \subseteq [2n]} \hat{g}(S) \chi_S(x) \right)\right] \\
&\leq \sum_{S \subseteq [2n]} |\hat{g}(S)| \cdot \left| \mathbb{E}_x[\mathrm{IP}_{2n}(x) \chi_S(x)] \right| \\
&\leq \sum_{S \subseteq [2n]} |\hat{g}(S)| \cdot \left| \widehat{\mathrm{IP}}_{2n}(S) \right| = \sum_{S \subseteq [2n]} |\hat{g}(S)| \cdot \frac{1}{2^n} \leq (1+\epsilon) \cdot \mathrm{rk}_\oplus(g) \cdot \frac{1}{2^n},
\end{aligned}$$

where we used the fact that $\widehat{\mathrm{IP}}_{2n}(S) = \frac{1}{2^n}$ for all $S \subseteq [2n]$, and $|\hat{g}(S)| \leq 1 + \epsilon$, since $|g(x)| \leq 1 + \epsilon$ for all $x \in \{0,1\}^{2n}$.

Note that on the other hand $\langle \mathrm{IP}_{2n}, g \rangle = \mathbb{E}_x[\mathrm{IP}_{2n}(x) g(x)] \geq 1 - \epsilon$. Combining this with the inequality above, we get

$$\mathrm{rk}_\oplus(g) \geq 2^n \cdot \frac{1-\epsilon}{1+\epsilon}.$$

□

Chapter 5

XOR-functions

Recall that the XOR-lift of a function $f : \{0,1\}^n \to \{0,1\}$ is defined as $F_\oplus : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ with $F_\oplus : (x, y) \mapsto f(x \oplus y)$.

Since XOR-lift is special case of the group lift for $G = \mathbb{Z}_2^n$, by Theorem 4.17, both Conjecture II, and Conjecture III are true for XOR functions.

5.1 Structure for bounded query complexity

Let $f : \{0,1\}^n \to \{0,1\}$, and consider the complexity measures

$$\mathrm{rdt}^{\oplus}(f) \le \mathrm{rdt}^{\oplus 1}(f) \le 3\,\mathrm{rdt}_0^{\oplus}(f),$$

and $\mathrm{dt}^{\oplus}(f)$. We shall study the structure of the function if we assume a uniform bound on each of these measures.

Deterministic and zero-error randomized case. The Fourier spectrum of a Boolean function plays an important role in understanding these parameters. The *Fourier rank* of f, denoted $\mathrm{rk}_\oplus(f)$, is simply the number of non-zero Fourier coefficients of f. The Fourier rank is also commonly referred to as Fourier sparsity in literature. Note that denoting $G = \mathbb{Z}_2^n$, using the notation of Definition 2.9, we have

$$\mathrm{rk}_\oplus(f) = \mathrm{rk}(\widehat{G}, f).$$

Proposition 5.1 (Equivalence between zero-error and deterministic complexities)**.** *For* $f : \{0,1\}^n \to \{0,1\}$, $\mathrm{D}(F_\oplus)$, $\mathrm{rk}(F_\oplus)$, $\mathrm{R}_0(F_\oplus)$, $\mathrm{dt}^\oplus(f)$, $\mathrm{rk}_\oplus(f)$, *and* $\mathrm{rdt}_0^\oplus(f)$ *are qualitatively equivalent. More precisely, we have*

$$\frac{1}{2}\log \mathrm{rk}_\oplus(f) \leq \mathrm{dt}^\oplus(f) \leq \mathrm{rk}_\oplus(f), \tag{5.1}$$

and there are constants $c_1, c_2, c_3 > 0$ *such that*

$$\mathrm{D}(F_\oplus) \leq 2\,\mathrm{dt}^\oplus(f) \leq c_1 \cdot \mathrm{D}(F_\oplus)^6 \leq c_2 \cdot \mathrm{rk}(F_\oplus)^6 \leq 2^{2^{c_3 \cdot \mathrm{R}_0(F_\oplus)}} \leq 2^{2^{2c_3\,\mathrm{rdt}_0^\oplus(f)}} \leq 2^{2^{2c_3\,\mathrm{dt}^\oplus(f)}}. \tag{5.2}$$

Proof. Equation (5.1): Each parity query $\oplus_{i\in S} x_i$ corresponds to querying the value of the corresponding character $\chi_S(x)$. In particular, if the Fourier spectrum of f is supported on at most c characters, then the value of $f(x)$ will be determined from the value of these characters, and thus $\mathrm{dt}^\oplus(f) \leq \mathrm{rk}_\oplus(f)$.

For the other direction, the indicator function of every leaf of a depth d parity decision tree is determined by the value of d characters and thus has Fourier rank at most 2^d. Since the number of leaves is bounded by 2^d, we obtain $\mathrm{rk}_\oplus(f) \leq 2^{2d}$.

Equation (5.2): The first inequality is the straightforward simulation of a parity decision tree by a communication protocol as discussed in Section 2.3, namely the fact that Alice and Bob can simulate an XOR-query $\oplus_S(x \oplus y)$ by two bits of communication $\oplus_S(x)$ and $\oplus_S(y)$. The second inequality is the parity lifting theorem of [HHL18], and the third inequality is a property of deterministic communication complexity Proposition 2.3. The fourth inequality is Theorem 4.7. The fifth inequality is again the simulation of parity decision trees by communication protocols. The final inequality is trivial since $\mathrm{rdt}_0^\oplus(f) \leq \mathrm{dt}^\oplus(f)$. □

Remark. To prove the equivalences stated in Proposition 5.1, instead of $\mathrm{dt}^\oplus(f) \leq c_1 \cdot \mathrm{D}(F_\oplus)^6$, it would have sufficed to use the weaker but trivial inequality $\mathrm{dt}^\oplus(f) \leq \mathrm{rk}_\oplus(f) = \mathrm{rk}(F_\oplus) \leq 2^{\mathrm{D}(F_\oplus)}$. However, the lifting theorem of [HHL18] provides stronger bounds.

One-sided randomized case. In Lemma 3.3 we saw that for a fixed integer k, the threshold function thr_k satisfies $\mathrm{rdt}^{\oplus 1}(\mathrm{thr}_k) \leq c_k$ for some constant c_k depending on parameter k, while $\mathrm{dt}^{\oplus}(\mathrm{thr}_k) = \Omega(n)$. This shows that for XOR-query model the one-sided error case is not qualitatively equivalent to the zero-error and the deterministic case.

Proposition 5.2. *For every Boolean function $f : \{0,1\}^n \to \{0,1\}$, there exists an affine subspace V of co-dimension $\mathrm{rdt}^{\oplus 1}(f)$ such that f is constant on V.*

Proof. Consider a one-sided randomized parity decision tree A_R with randomness R that could only make errors when $f(x) = 1$. Suppose that $f \not\equiv 0$, as otherwise we can take $V = \{0,1\}^n$. Pick $x \in f^{-1}(1)$. Since $\Pr_R[A_R(x) = 1] > 0$, there is a fixing of randomness $R = r$, such that A_r is a deterministic parity decision tree satisfying $A_r(x) = 1$. That is, x leads to a leaf of A_r labeled with 1, and the leaf corresponds to an affine subspace V of codimension $\leq \mathrm{rdt}^{\oplus 1}(f)$. Moreover, since A_r does not make errors on $f^{-1}(0)$, then $V \cap f^{-1}(0) = \emptyset$ or, equivalently, $f|_V \equiv 1$. □

Two-sided error case. Next we turn to two-sided error. We saw in Corollary 2.16 that the randomized parity decision tree complexity and the approximate Fourier algebra norm of f are qualitatively equivalent. These parameters are also qualitatively equivalent to the randomized communication complexity of the parity lift.

Proposition 5.3. *For $f : \{0,1\}^n \to \{0,1\}$ and $\epsilon \in (0, \frac{1}{2})$, $\mathrm{R}_\varepsilon(F_\oplus)$, $\mathrm{rdt}_\epsilon^{\oplus}(f)$, and $\|f\|_{A,\varepsilon}$ are qualitatively equivalent. More precisely,*

$$\log \|f\|_{A,\varepsilon} \leq \mathrm{rdt}_\varepsilon^{\oplus}(f) \leq O\left(c_\epsilon \|f\|_{A,\varepsilon}^2\right), \tag{5.3}$$

$$\frac{1}{2} \log \|f\|_{A,\varepsilon} \leq \mathrm{R}_\epsilon(F_\oplus) \leq O\left(c_\epsilon \|f\|_{A,\varepsilon}^2\right), \tag{5.4}$$

where $c_\epsilon = \frac{\log(1/\varepsilon)}{(1-2\epsilon)^2}$, and

$$\mathrm{R}_\varepsilon(F_\oplus) \leq 2\,\mathrm{rdt}_\varepsilon^{\oplus}(f) \leq O\left(c_\epsilon 2^{4\,\mathrm{R}_\varepsilon(F_\oplus)}\right). \tag{5.5}$$

Proof. Observe that a parity lift is a $y^{-1}x$-group lift for $G = \mathbb{Z}_2^n$, and thus by Corollary 4.16, we have $\|F_\oplus\|_{\gamma_2,\varepsilon} = \|f\|_{A,\varepsilon}$. Hence Equation (5.3) and Equation (5.4) have already been proven in Corollary 2.16.

The first inequality in Equation (5.5) is the standard simulation of a parity decision tree by a communication protocol. The second inequality in Equation (5.5) is a direct consequence of the upper-bound in Equation (5.3) and the lower bound in Equation (5.4).

□

Remark. Note that Equation (5.3) provides an exponential lifting theorem for the randomized parity decision tree model. It is conjectured in [HHL18] that this can be improved to $\mathrm{rdt}^{\oplus}(f) \leq \mathrm{R}(F_{\oplus})^{O(1)}$, which remains an intriguing open problem.

Remark. The counter-example to the log-approximate-rank conjecture [CMS20] demonstrates that the upper bound both in Equation (5.3) and Equation (5.4) is almost tight. Let $\mathrm{SINK} : \{0,1\}^{\binom{m}{2}} \to \{0,1\}$ be a function where the input specifies the orientation of every edge in the complete directed graph on m vertices, and SINK outputs 1 if there is a vertex that is a sink, it outputs 0 otherwise. It is proven in [CMS20] that $\| \mathrm{SINK} \|_{A,\varepsilon} \leq \| \mathrm{SINK} \|_{A} \leq m$ and $\mathrm{rdt}^{\oplus}(\mathrm{SINK}) = \mathrm{R}(\mathrm{SINK}_{\oplus}) = \Theta(m)$.

It follows from Equation (5.3) that Conjecture IV has the following equivalent form:

Conjecture 5.4. *Let $f : \mathbb{Z}_2^n \to \{0,1\}$ be a Boolean function such that $\mathrm{rdt}_{\varepsilon}^{\oplus}(f) \leq c$. Then there exists a coset $V = H + a \subseteq \mathbb{Z}_2^n$ such that f is constant on V, and $\frac{|V|}{|\mathbb{Z}_2^n|} \geq \delta_c > 0$, where $\delta_c > 0$ is a constant that only depends on c.*

Next, we observe that for the class of XOR-functions, Conjecture IV would imply Conjecture I.

Proposition 5.5. *For the class of* XOR *functions,*

$$\textit{Conjecture IV} \Rightarrow \textit{Conjecture I}.$$

Proof. Suppose that $\mathrm{R}(F_{\oplus}) \leq c$. It follows then from Equation (5.4) that

$$\|f\|_{A,\epsilon} \leq 2^{2c}.$$

Now if Conjecture IV is true, then f would be constant on a large subspace $V \subseteq \mathbb{Z}_2^n$. Then $V \times V$ would be a large monochromatic rectangle in $F_{\oplus}$. □

Chapter 6

AND-functions

In this section we focus on AND-functions $F_\wedge(x,y) \coloneqq f(x \wedge y)$. As we saw in Chapter 5, investigating the Fourier expansion of $f : \{0,1\}^n \to \{0,1\}$ was extremely useful for understanding the properties of their XOR -lifts. This is chiefly because Fourier characters are multiplicative with respect to the XOR operation, and thus the Fourier transform naturally translates to an expansion of the matrix $F_\oplus$ as a linear combination of rank-one matrices. When studying the AND-lifts, the representation of f as a multilinear polynomial over the reals plays a similar role since monomials are multiplicative with respect to the AND operation. More precisely, using the notation $x^S = \prod_{i\in S} x_i$, the polynomial representation

$$f(x) = \sum_{S\subseteq[n]} \lambda_S x^S,$$

translates to

$$F_\wedge(x,y) = f(x \wedge y) = \sum_{S\subseteq[n]} \lambda_S x^S y^S.$$

Equivalently,

$$F_\wedge = \sum_{S\subseteq[n]} \lambda_S m_S m_S^{\mathrm{T}},$$

where $m_S \in \{0,1\}^{2^n}$, m_S^{T} is the transform of m_S, and $(m_S)_x = x^S$. Since for each S, $m_S m_S^{\mathrm{T}}$ is a rank-1 matrix, and m_S for $S \subseteq [n]$ are linearly independent, then $\mathrm{rk}(F_\wedge)$ is equal to the number of non-zero coefficients λ_S, which by the notation of Section 2.4 is denoted by

$\mathrm{rk}(\mathcal{Mon}, f)$. In other words,

$$\mathrm{rk}(F_\wedge) = \mathrm{rk}(\mathcal{Mon}, f). \tag{6.1}$$

We obtain the following simple proposition, which establishes the equivalence of several parameters related to the AND-lift.

Proposition 6.1 (Equivalence between zero-error and deterministic complexities)**.** *For $f : \{0,1\}^n \to \{0,1\}$, the parameters $\mathrm{dt}^\wedge(f)$, $\mathrm{rdt}_0^\wedge(f)$, $\mathrm{rk}(\mathcal{Mon}, f)$, $\|f\|_{\mathcal{Mon}}$, $\mathrm{rk}(F_\wedge)$, $\mathrm{D}(F_\wedge)$, and $\mathrm{R}_0(F_\wedge)$ are all qualitatively equivalent. More precisely, there exists a constant $c > 0$ such that*

$$\begin{aligned}\log \mathrm{rk}(\mathcal{Mon}, f) \le \mathrm{D}(F_\wedge) \le 2\,\mathrm{dt}^\wedge(f) \le 2\mathrm{rk}(\mathcal{Mon}, f)&\\ = 2\mathrm{rk}(F_\wedge) \le 2^{2^{c\,\mathrm{R}_0(F_\wedge)}} \le 2^{2^{2c\cdot\mathrm{rdt}_0^\wedge(f)}} \le 2^{2^{2c\cdot\mathrm{rk}(\mathcal{Mon}, f)}},&\end{aligned} \tag{6.2}$$

and

$$\mathrm{rk}(\mathcal{Mon}, f) \le \|f\|_{\mathcal{Mon}} \le 3^{\mathrm{dt}^\wedge(f)}.$$

Proof. Recall $\mathrm{rk}(F_\wedge) = \mathrm{rk}(\mathcal{Mon}, f)$. Thus the inequality $\log \mathrm{rk}(\mathcal{Mon}, f) \le \mathrm{D}(F_\wedge)$ is the well-known rank lower bound of Proposition 2.3, and the inequality $\mathrm{D}(F_\wedge) \le 2\,\mathrm{dt}^\wedge(f)$ is the straightforward simulation of an AND-decision tree by a communication protocol, discussed in Section 2.3.

The inequality $\mathrm{dt}^\wedge(f) \le \mathrm{rk}(\mathcal{Mon}, f)$ follows from the fact that the value of a monomial can be determined by making one AND-query.

By Theorem 4.7, there exists a constant $c > 0$ such that

$$\mathrm{rk}(F_\wedge) \le 2^{2^{c\,\mathrm{R}_0(F_\wedge)}} \le 2^{2^{2c\,\mathrm{rdt}_0^\wedge(f)}},$$

and the last inequality in the first equation follows from $\mathrm{R}_0(F_\wedge) \le 2\,\mathrm{rdt}_0^\wedge(f) \le 2\,\mathrm{dt}^\wedge(f) \le 2\mathrm{rk}(\mathcal{Mon}, f)$.

The inequality $\mathrm{rk}(\mathcal{Mon}, f) \le \|f\|_{\mathcal{Mon}}$ follows from the easy and well-known fact that the coefficients in the polynomial representation of f are all integers.

It remains to prove $\|f\|_{\mathcal{Mon}} \le 3^{\mathrm{dt}^\wedge(f)}$. We use induction on $d = \mathrm{dt}^\wedge(f)$. The base case for $d = 0$ is trivial, as $\|f\|_{\mathcal{Mon}}$ is at most 1 for every constant Boolean function f. For the induction step, consider an AND-decision tree of depth d computing f, and suppose that the top node of the tree queries x^S, and branches accordingly to compute f_1 and f_2. Now

$$f(x) = x^S \cdot f_1(x) + (1 - x^S) \cdot f_2(x),$$

and since $\mathrm{dt}^\wedge(f_1), \mathrm{dt}^\wedge(f_2) \leq d - 1$, we have

$$\|f\|_{\mathcal{Mon}} \leq \|x^S f_1\|_{\mathcal{Mon}} + \|x^S f_2\|_{\mathcal{Mon}} + \|f_2\|_{\mathcal{Mon}} \leq 3 \cdot 3^{d-1} = 3^d.$$

□

We conjecture that the exponential equivalence between $\mathrm{D}(F_\wedge)$ and $\mathrm{dt}^\wedge(f)$ in Proposition 6.1 can be improved to a polynomial equivalence. Recently, [KLMY20] proved $\mathrm{dt}^\wedge(f) = O(\mathrm{D}(f_\wedge)^3 \log n)$, but due to the $\log(n)$ factor, their statement comes short of establishing this conjecture.

Now, let us turn to randomized communication complexity and its related matrix parameters such as the trace and the γ_2 norm. Unlike Fourier characters, the monomials in the polynomial representation are not orthogonal, and thus the coefficients in the polynomial representation of f do not correspond to the eigenvalues of $F_\wedge$. This makes relating the spectral properties of $F_\wedge$ to similar properties of f difficult. For example, unlike the $F_\oplus$ case, we do not know how to verify Conjecture II or Conjecture III for matrices of the form $F_\wedge$. Similarly, we do not know how to relate the randomized communication complexity assumption of Conjecture I to an assumption about $\mathrm{rdt}^\wedge$. Contrast this with the XOR case where we have established that $\mathrm{R}(F_\oplus)$, $\|F_\oplus\|_{\gamma_2,\epsilon}$, $\|f\|_{A,\epsilon}$, and $\mathrm{rdt}_\oplus(f)$ are all qualitatively equivalent. We conjecture however that a similar statement is true for the AND-functions.

Conjecture 6.2. *There exist an increasing function $\kappa : \mathbb{R}^+ \to \mathbb{R}^+$ such that for every $f : \{0,1\}^n \to \{0,1\}$,*

$$\mathrm{rdt}^\wedge(f) \leq \kappa(\mathrm{R}(F_\wedge)).$$

Interestingly in the case of the AND-functions, we know how to establish the analogue of Conjecture IV.

Theorem 6.3. *Suppose $f : \{0,1\}^n \to \{0,1\}$ satisfies $\mathrm{rdt}^\wedge(f) \leq d$. Then, there exists a set $J \subseteq [n]$ of size at most 3^{d+1}, such that f is constant on $\{x : x_J = \mathbf{0}\}$.*

We will prove Theorem 6.3 in Section 6.1, but first, let us state the following corollary.

Corollary 6.4. *Conjecture 6.2, if true, would imply that Conjecture I is true for $F_\wedge$ matrices.*

Proof. It would follow from Conjecture 6.2 that if $\mathrm{R}(F_\wedge) \leq c$, then $\mathrm{rdt}^\wedge(f) \leq \kappa(c)$. Then by Theorem 6.3, f is constant on $V = \{x : x_J = \mathbf{0}\}$, where $|J| \leq 3^{\kappa(c)+1}$. Consequently, $F_\wedge$ is constant on $V \times V$, which is a $\delta 2^n \times \delta 2^n$ combinatorial rectangle with $\delta = 2^{-|J|} \geq 2^{-3^{\kappa(c)+1}}$. □

To summarize, in the case of $F_\wedge$, the missing step for establishing Conjecture I is a dimension-free lifting theorem for randomized communication complexity (i.e. Conjecture 6.2), since we know how to deduce structure from a uniform bound on randomized query complexity. In contrast, in the case of $F_\oplus$ such a lifting theorem is known, but we do not know how to establish structure from a uniform bound on randomized query complexity (i.e. Conjecture IV).

6.1 Proof of Theorem 6.3

By Corollary 2.16,

$$\log_3 \|f\|_{\mathcal{Mon},\varepsilon} \leq \mathrm{rdt}^\wedge_\varepsilon(f) \leq O\left(\|f\|^2_{\mathcal{Mon},\varepsilon} \cdot \frac{\log(1/\varepsilon)}{(1-2\epsilon)^2}\right). \tag{6.3}$$

Theorem 6.3 now follows from the first inequality and the following lemma.

Lemma 6.5. *For every $f : \{0,1\}^n \to \{0,1\}$, there exists a set $J \subseteq [n]$ of size at most $3\|f\|_{\mathcal{Mon},1/3}$, such that f is constant on $\{x : x_J = \mathbf{0}\}$.*

Proof. Let $p = \sum_{S \subseteq [n]} \lambda_S x^S$ be a multilinear polynomial satisfying $\|p - f\|_\infty \leq \frac{1}{3}$ and $\|p\|_{\mathcal{Mon}} = d$.

Consider the partial ordering on the Boolean cube where $x \preceq y$ if for every i, $x_i \leq y_i$. Under this ordering, pick a minimal $w \in \{0,1\}^n$ such that $f(\mathbf{0}) \neq f(w)$. This means that for every $v \prec w$, $f(v) = f(\mathbf{0})$. Pick an arbitrary j such that $w_j = 1$, and let $v = w - \mathbf{e}_j$, where $\mathbf{e}_j$ denotes the j-th standard vector. Note that $|f(w) - f(v)| = 1$, and as a result $|p(w) - p(v)| \geq 1/3$, which means that

$$\sum_{S \subseteq w : S \ni j} |\lambda_S| \geq \frac{1}{3},$$

where $S \subseteq w$ means $S \subseteq \{i : w_i = 1\}$. Consequently, $\|p|_{x_j=0}\|_{\mathcal{Mon}} \leq \|p\|_{\mathcal{Mon}} - \frac{1}{3}$. Thus

$$\|f|_{x_j=0}\|_{\mathcal{Mon},1/3} \leq \|f\|_{\mathcal{Mon},1/3} - \frac{1}{3}.$$

We include j in J and repeat the above process, replacing f with $f|_{x_j=0}$. Since $\|\cdot\|_{\mathcal{Mon},1/3} \geq 0$, this process can be repeated for at most $3\|f\|_{\mathcal{Mon},1/3}$ times, after which we will end up with a constant function. □

6.2 Randomized AND-decision trees: One-sided and two-sided error

Let us briefly discuss $\mathrm{rdt}^{\wedge 1}$ and $\mathrm{rdt}^{\wedge}$. The example of the threshold function, as discussed in Lemma 3.4, shows that the one-sided and the two-sided error case are not qualitatively equivalent to the deterministic case. In particular, for $f = \overline{\mathrm{thr}}_{n-1}$, Lemma 3.4 shows that

$$\mathrm{R}(F_\wedge) \leq 2\,\mathrm{rdt}^\wedge(f) \leq 2\,\mathrm{rdt}^{\wedge 1}(f) = O(1), \qquad \text{while} \qquad \mathrm{dt}^\wedge(f) = \mathrm{dt}^\wedge(\overline{f}) = \Omega(\log(n)).$$

On the other hand, in Theorem 6.3, we showed that if $\mathrm{rdt}^\wedge(f) \leq d$, then there exists a set $J \subseteq [n]$ of size at most 3^{d+1}, such that f is constant on $\{x : x_J = \mathbf{0}\}$. Thus for AND-functions we know how to prove the analogue of Proposition 5.2, even for two-sided error.

Chapter 7

Forbidden substructures: A proof-barrier for Conjectures I, II, III

In this section, we discuss a proof barrier, which shows that the techniques used for proving Cohen's idempotent theorem, as well as many similar structural results cannot establish Conjectures I, II, and III. Such proofs are based on forbidding substructures. For instance, to prove Cohen's idempotent theorem for $f : \mathbb{Z}_2^n \to \{0,1\}$, one uses the fact that the function $g_r : \mathbb{Z}_2^r \to \{0,1\}$, defined as $g_r(x) = 1$ iff $|x| = 1$, satisfies $\|g_r\|_A = \Omega(\sqrt{r})$. Consequently, if $\|f\|_A \leq c$, then no restriction of f to any affine subspace of dimension $k = k_c = O(c^2)$ can be isomorphic to g_k. One then uses the fact that f does not have a copy of this forbidden substructure to obtain general structural results about f. The proof of Cohen's theorem, even for more general groups, follows the same approach.

Similarly, in Lemma 4.6, we showed that every Boolean matrix of high rank must contain as a submatrix one of the four matrices $\mathtt{I}_k$, $\overline{\mathtt{I}}_k$, GT_k, or $\overline{\mathrm{GT}}_k$, each with large zero-error randomized communication complexity. In other words, we used these four matrices as forbidden substructures for matrices that have small zero-error randomized communication complexity. For one-sided error, in Theorem 4.10 we used the forbidden matrix $\mathtt{I}_k$. Note that even Sherstov's pattern-matrix method [She11], which has been used successfully to lower-bound several complexity measures of various important matrices, is based on finding certain highly symmetric patterns in them.

One may suspect that a similar approach could also be used to establish Conjectures I, II, and III. Namely, one needs to find a suitable list of matrices with high randomized communication complexity, high trace norm, or high γ_2 norm, and show that if a Boolean matrix M does not contain any of them as a submatrix, then it must have the desired structure. We prove that this approach fails as there are matrices that cannot be handled by this proof technique.

Theorem 7.1. *For every sufficiently large n, there exists an $n \times n$ Boolean matrix M with the following properties.*

(i) Every $n^{1/4} \times n^{1/4}$ submatrix F of M satisfies

$$\|F\|_{\mathrm{ntr}} \leq \|F\|_{\gamma_2} \leq 4, \ \textit{and} \quad \mathrm{R}(F) = O(1).$$

(ii) M does not contain any monochromatic rectangles of size $n^{0.99} \times n^{0.99}$.

One interesting related proof that does not follow the forbidden substructure approach is the purely spectral proof of Shpilka, Tal, and Volk [STV17] for the fact that every $f : \mathbb{Z}_2^n \to \{0,1\}$ with $\|f\|_A \leq c$ is constant on an affine subspace of co-dimension k_c. This obviously follows from Cohen's theorem, but [STV17] obtained stronger bounds on k_c.

Before stating the proof of Theorem 7.1, we will set up and prove an auxiliary lemma on the blocky-rank of matrices that correspond to forests. A matrix $M : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ naturally corresponds to a bipartite graph G_M with bipartition $\mathcal{X} \cup \mathcal{Y}$, where there is an edge between vertices $x \in \mathcal{X}$ and $y \in \mathcal{Y}$ if and only if $M(x,y) = 1$. Note that the bipartite graph corresponding to a blocky matrix M is an edge-disjoint union of vertex-disjoint complete bipartite graphs.

Recall that a graph is called a *forest* if it does not contain any cycles. A connected forest is called a *tree*. Recall that both a tree and a forest are bipartite graphs.

Lemma 7.2. *Let M be a finite Boolean matrix corresponding to a forest. Then M is a sum of two blocky matrices.*

Proof. As mentioned above, a blocky matrix corresponds to an edge-disjoint union of vertex-disjoint complete bipartite graphs. Hence it suffices to show that the edges of every forest can be partitioned into two sets, each forming a disjoint union of complete bipartite graphs. Obviously, it suffices to prove this for a tree as a forest is a disjoint union of trees. Let v be an arbitrary vertex of the tree, and for $i = 0, 1, \ldots$, let L_i be the set of the vertices that are within distance i from v. To complete the proof note that the edges between L_i and L_{i+1} for even values of i form one blocky matrix, and similarly the edges between L_i and L_{i+1} for odd values of i form the other blocky matrix. □

Proof of Theorem 7.1. Set $p = \frac{n^{0.01}}{n}$, and select a random $n \times n$ matrix $M = [m_{ij}]$ by setting each entry to 1 with probability p and independently of other entries. It suffices to show that with probability $1 - o(1)$ both (i) and (ii) hold.

(i) Let $k = n^{1/4}$. We will show that every $k \times k$ submatrix F of M can be written as a sum of four blocky matrices. Then $\mathrm{R}(F) = O(1)$ immediately follows from Equation (4.3), and $\|F\|_{\mathrm{ntr}} \leq \|F\|_{\gamma_2} \leq 4$ follows from the fact that the γ_2-norm of a blocky matrix is at most 1.

We first prove that with probability $1 - o(1)$, for every $r, t \leq k$, every $r \times t$ submatrix of M contains a row or a column with at most two 1's. Note that the statement is trivial when $\min(r, t) \leq 2$. Fix $r, t > 2$, and assume without loss of generality that $r \leq t$. The probability that there is an $r \times t$ submatrix such that each of its t columns contains at least three 1's is bounded by

$$\binom{n}{r}\binom{n}{t}\left(\binom{r}{3}p^3\right)^t \leq n^r n^t (r^3 p^3)^t \leq (n^2 p^3 t^3)^t \leq \left(\frac{n^{0.03}}{n^{1/4}}\right)^t \leq o(n^{-1/2}).$$

Thus by a union bound over all choices of $r, t \leq k$, the probability that there is $r, t \in [k]$ and an $r \times t$ submatrix where every column contains at least three 1's is bounded by $o(k^2 n^{-1/2})$ which is $o(1)$ as desired.

Now suppose that every $r \times t$ submatrix F of M contains a row or a column with at most two 1's. We will show that in this case, every such F is a disjoint union of two forests, and by Lemma 7.2 M is a sum of four blocky matrices. Consider a row (or a column) with at most two 1's, and let e_1 and e_2 be the edges corresponding to these (at most) two entries. Removing this row from F will result in a smaller submatrix, which by induction hypothesis, can be written as the union of two forests $\mathcal{F}_1$ and $\mathcal{F}_2$. Now F can be decomposed into the union of two forests $\mathcal{F}_1 \cup \{e_1\}$ and $\mathcal{F}_2 \cup \{e_2\}$. Note that in the base case, i.e. when $r = 1$ or $t = 1$ we get a star, which itself is a tree.

(ii) Let $K = n^{0.99}$. The expected number of monochromatic rectangles of size $K \times K$ is at most

$$2^n \times 2^n \times \left(p^{K^2} + (1-p)^{K^2}\right) \leq 2^{2n}(2e^{-pK^2}) \leq 2^{3n-pK^2} = 2^{3n-n^{1.98+0.01}} = o(1).$$

□

Lastly, it is worth mentioning that the matrix M from Theorem 7.1 is not a counterexample for Conjecture I as M in fact has a high randomized communication complexity – this can be derived by upper bounding M's discrepancy.

In a follow up work to this thesis, Hambardzumyan, H. Hatami, P. Hatami [HHH21] showed that Theorem 7.1 provides a counterexample to the Probabilistic Universal Graph Conjecture of Harms, Wild, and Zamaraev [HWZ21]. Later work of H. Hatami and P. Hatami [HH21], based on the idea of Theorem 7.1 refuted the Implicit Graph Conjecture itself.

Chapter 8

Conclusion and Summary

To summarize the results of this thesis and to point out the open problems below we bring Figure 8.1 and Figure 8.2. The first figure focuses on Conjectures I, II, III, IV and it records our progress towards resolving each one of them for general functions, lifted functions, XOR-functions and AND-functions.

Conjectures		$F : \mathcal{X} \times \mathcal{Y} \to \{0, 1\}$	$F(x, y) = f(y^{-1}x)$	XOR-functions	AND-functions
Conjecture I	R	open	open	open	open
	R_1	Theorem 4.10	–	–	–
	R_0	Theorem 4.7	–	–	–
Conjecture II		open	Theorem 4.17	–	open
Conjecture III		open (Equivalent to Conjectures 4.2, 4.11)	Theorem 4.17	–	open
Conjecture IV		open (weaker version Proposition 4.18)	open (implies Conjecture I)	open (Equivalent to Conjecture 5.4)	open (Analogous to Theorem 6.3)

Figure 8.1: Summary of some of the results and conjectures. The dash (–) denotes that the corresponding result trivially follows from the result in the previous column (same row).

The next figure focuses on the second theme of the thesis – qualitative equivalence. It indicates all the known (qualitative) equivalences between measures that appeared and/or are proven in this work.

$$\mathrm{D}^{\mathrm{EQ}}(M) \xleftrightarrow{\text{Prop. 4.1}} \mathrm{rk}(\mathcal{Blocky}, M) \xleftrightarrow{\text{Conj. 4.2}} \|M\|_{\mathcal{Blocky}}$$

$$\mathrm{R}_0(M) \xleftrightarrow{\text{Thm. 4.7}} \mathrm{rk}_{\varepsilon}(M) \xleftrightarrow{\text{Thm. 4.8}} \mathrm{rk}(M) \xleftrightarrow{\text{Eq. 1.4}} \mathrm{D}(M)$$

$$\mathrm{rdt}_0^{\oplus}(f) \xleftrightarrow{\text{Prop. 5.1}} \mathrm{R}_0(F_{\oplus}) \xleftrightarrow{\text{Prop. 5.1}} \mathrm{rk}(F_{\oplus}) \xleftrightarrow{\text{Eq. 1.4}} \mathrm{D}(F_{\oplus}) \xleftrightarrow{\text{Prop. 5.1}} \mathrm{dt}^{\oplus}(f) \xleftrightarrow{\text{Eq. 5.1}} \mathrm{rk}_{\oplus}(f)$$

$$\mathrm{rdt}_{\varepsilon}^{\oplus}(f) \xleftrightarrow{\text{Prop. 5.3}} \|f\|_{A,\varepsilon} \xleftrightarrow{\text{Prop. 5.3}} \mathrm{R}_{\varepsilon}(F_{\oplus})$$

$$\mathrm{rdt}_0^{\wedge}(f) \xleftrightarrow{\text{Prop. 6.1}} \mathrm{R}_0(F_{\wedge}) \xleftrightarrow{\text{Prop. 6.1}} \mathrm{D}(F_{\wedge}) \xleftrightarrow{\text{Prop. 6.1}} \mathrm{dt}^{\wedge}(f) \xleftrightarrow{\text{Prop. 6.1}} \mathrm{rk}(\mathcal{Mon}, f) \xleftrightarrow{\text{Prop. 6.1}} \|f\|_{\mathcal{Mon}}$$

$$\mathrm{rdt}^{\wedge}(f) \xleftrightarrow{\text{Eq. 6.3}} \|f\|_{\mathcal{Mon},\varepsilon} \xleftrightarrow{\text{Conj. 6.2}} \mathrm{R}(F_{\wedge}).$$

Figure 8.2: Denote by $A \leftrightarrow B$ if A and B are qualitatively equivalent, meaning $\exists \kappa_1, \kappa_2 : \mathbb{R}_+ \to \mathbb{R}_+$ such that $A \leq \kappa_1(B)$ and $B \leq \kappa_2(A)$. M is a Boolean matrix, $f : \{0,1\}^n \to \{0,1\}$ is a Boolean function, $F_{\oplus}$ and $F_{\wedge}$ denote the XOR and AND-lifts of f, respectively. The red arrow indicates that equivalence is not known and is conjectured.

Bibliography

[Alo86] Noga Alon. Covering graphs by the minimum number of equivalence relations. *Combinatorica*, 6(3):201–206, 1986.

[Alo09] Noga Alon. Perturbed identity matrices have high rank: proof and applications. *Combin. Probab. Comput.*, 18(1-2):3–15, 2009.

[BFS86] László Babai, Peter Frankl, and Janos Simon. Complexity classes in communication complexity theory. In *27th Annual Symposium on Foundations of Computer Science (sfcs 1986)*, pages 337–347. IEEE, 1986.

[BH04] William D. Banks and Asma Harcharras. On the norm of an idempotent Schur multiplier on the Schatten class. *Proc. Amer. Math. Soc.*, 132(7):2121–2125, 2004.

[BK95] Aart Blokhuis and Ton Kloks. On the equivalence covering number of splitgraphs. *Information Processing Letters*, 54(5):301–304, 1995.

[BN07] Béla Bollobás and Vladimir Nikiforov. Cliques and the spectral radius. *Journal of Combinatorial Theory, Series B*, 97(5):859–865, 2007.

[Chu14] Maria Chudnovsky. The Erdös-Hajnal conjecture—a survey. *J. Graph Theory*, 75(2):178–190, 2014.

[CKLM19] Arkadev Chattopadhyay, Michal Kouckỳ, Bruno Loff, and Sagnik Mukhopadhyay. Simulation theorems via pseudo-random properties. *computational complexity*, 28(4):617–659, 2019.

[CLV19] Arkadev Chattopadhyay, Shachar Lovett, and Marc Vinyals. Equality alone does not simulate randomness. In *34th Computational Complexity Conference (CCC 2019)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2019.

[CMS20] Arkadev Chattopadhyay, Nikhil S. Mande, and Suhail Sherif. The log-approximate-rank conjecture is false. *J. ACM*, 67(4):Art. 23, 28, 2020.

[Coh60] Paul J. Cohen. On a conjecture of Littlewood and idempotent measures. *Amer. J. Math.*, 82:191–212, 1960.

[CR12] Amit Chakrabarti and Oded Regev. An optimal lower bound on the communication complexity of gap-Hamming-distance. *SIAM J. Comput.*, 41(5):1299–1317, 2012.

[DD07] Kenneth R. Davidson and Allan P. Donsig. Norms of Schur multipliers. *Illinois J. Math.*, 51(3):743–766, 2007.

[Duc79] Pierre Duchet. *Représentations, noyaux en théorie des graphes et hypergraphes.* PhD thesis, 1979.

[ELT16] G. K. Eleftherakis, R. H. Levene, and I. G. Todorov. Schur idempotents and hyperreflexivity. *Israel J. Math.*, 215(1):317–337, 2016.

[Eym64] Pierre Eymard. L'algèbre de Fourier d'un groupe localement compact. *Bull. Soc. Math. France*, 92:181–236, 1964.

[For02] Jürgen Forster. A linear lower bound on the unbounded error probabilistic communication complexity. volume 65, pages 612–625. 2002. Special issue on complexity, 2001 (Chicago, IL).

[Fra82] Péter Frankl. Covering graphs by equivalence relations. In *North-Holland Mathematics Studies*, volume 60, pages 125–127. Elsevier, 1982.

[GKPW17] Mika Göös, Pritish Kamath, Toniann Pitassi, and Thomas Watson. Query-to-communication lifting for P^{NP}. 79:Art. No. 12, 16, 2017.

[GLM$^+$16] Mika Göös, Shachar Lovett, Raghu Meka, Thomas Watson, and David Zuckerman. Rectangles are nonnegative juntas. *SIAM Journal on Computing*, 45(5):1835–1869, 2016.

[GN08] C. D. Godsil and M. W. Newman. Eigenvalue bounds for independent sets. *J. Combin. Theory Ser. B*, 98(4):721–734, 2008.

[GPW18a] Mika Göös, Toniann Pitassi, and Thomas Watson. Deterministic communication vs. partition number. *SIAM J. Comput.*, 47(6):2435–2450, 2018.

[GPW18b] Mika Göös, Toniann Pitassi, and Thomas Watson. The landscape of communication complexity classes. *Comput. Complexity*, 27(2):245–304, 2018.

[GPW20] Mika Göös, Toniann Pitassi, and Thomas Watson. Query-to-communication lifting for BPP. *SIAM J. Comput.*, 49(4):441–461, 2020.

[Gro52] A. Grothendieck. Résumé des résultats essentiels dans la théorie des produits tensoriels topologiques et des espaces nucléaires. *Ann. Inst. Fourier (Grenoble)*, 4:73–112 (1954), 1952.

[GS08] Ben Green and Tom Sanders. A quantitative version of the idempotent theorem in harmonic analysis. *Ann. of Math. (2)*, 168(3):1025–1054, 2008.

[GS19] Anna Gál and Ridwan Syed. Upper bounds on communication in terms of approximate rank. In *Electronic Colloquium on Computational Complexity (ECCC)*, volume 26, page 6, 2019.

[HH21] Hamed Hatami and Pooya Hatami. The implicit graph conjecture is false. *arXiv preprint arXiv:2111.13198*, 2021.

[HHH21] Lianna Hambardzumyan, Hamed Hatami, and Pooya Hatami. A counterexample to the probabilistic universal graph conjecture via randomized communication complexity. *arXiv preprint arXiv:2111.10436*, 2021.

[HHL18] Hamed Hatami, Kaave Hosseini, and Shachar Lovett. Structure of protocols for XOR functions. *SIAM Journal on Computing*, 47(1):208–217, 2018.

[HMP86] B. Host, J.-F. Méla, and F. Parreau. Analyse harmonique des mesures. *Astérisque*, (135-136):261, 1986.

[HWZ21] Nathaniel Harms, Sebastian Wild, and Viktor Zamaraev. Randomized communication and the implicit graph conjecture. *CoRR*, abs/2111.03639, 2021.

[Juk06] Stasys Jukna. On graph complexity. *Comb. Probab. Comput.*, 15(6):855–876, 2006.

[Juk12] Stasys Jukna. *Boolean function complexity*, volume 27 of *Algorithms and Combinatorics*. Springer, Heidelberg, 2012. Advances and frontiers.

[KI40] Yukiyosi Kawada and Kiyosi Itô. On the probability distribution on a compact group. I. *Proc. Phys.-Math. Soc. Japan (3)*, 22:977–998, 1940.

[KLMY20] Alexander Knop, Shachar Lovett, Sam McGuire, and Weiqiang Yuan. Log-rank and lifting for AND-functions, 2020.

[KN97] Eyal Kushilevitz and Noam Nisan. *Communication complexity.* Cambridge University Press, Cambridge, 1997.

[KP05] Aristides Katavolos and Vern I. Paulsen. On the ranges of bimodule projections. *Canad. Math. Bull.*, 48(1):97–111, 2005.

[Kri79] J.-L. Krivine. Constantes de Grothendieck et fonctions de type positif sur les sphères. *Adv. in Math.*, 31(1):16–30, 1979.

[KS07] Adam R Klivans and Alexander A Sherstov. A lower bound for agnostically learning disjunctions. In *International Conference on Computational Learning Theory*, pages 409–423. Springer, 2007.

[Lef72] Marcel Lefranc. Sur certaines algèbres de fonctions sur un groupe. *C. R. Acad. Sci. Paris Sér. A-B*, 274:A1882–A1883, 1972.

[Lev14] Rupert H. Levene. Norms of idempotent Schur multipliers. *New York J. Math.*, 20:325–352, 2014.

[Liv95] Leo Livshits. A note on 0-1 Schur multipliers. *Linear Algebra Appl.*, 222:15–22, 1995.

[LLT07] Mei Lu, Huiqing Liu, and Feng Tian. Laplacian spectral bounds for clique and independence numbers of graphs. *Journal of Combinatorial Theory, Series B*, 97(5):726–732, 2007.

[Lov14] Shachar Lovett. Recent advances on the log-rank conjecture in communication complexity. *Bull. Eur. Assoc. Theor. Comput. Sci. EATCS*, (112):18–35, 2014.

[Lov16] Shachar Lovett. Communication is bounded by root of rank. *J. ACM*, 63(1):Art. 1, 9, 2016.

[LS07] Troy Lee and Adi Shraibman. Lower bounds in communication complexity. *Found. Trends Theor. Comput. Sci.*, 3(4):front matter, 263–399 (2009), 2007.

[LS09] Nati Linial and Adi Shraibman. Lower bounds in communication complexity based on factorization norms. *Random Structures & Algorithms*, 34(3):368–394, 2009.

[LSG12] Xueliang Li, Yongtang Shi, and Ivan Gutman. *Graph energy.* Springer, New York, 2012.

[Ḿ82] J.-F. Méla. Mesures ε-idempotentes de norme bornée. *Studia Math.*, 72(2):131–149, 1982.

[Mat93] Roy Mathias. The Hadamard operator norm of a circulant and applications. *SIAM J. Matrix Anal. Appl.*, 14(4):1152–1167, 1993.

[MO09] Ashley Montanaro and Tobias Osborne. On the communication complexity of XOR functions. *arXiv preprint arXiv:0909.3392*, 2009.

[MP16] Jayden Mudge and Hung Le Pham. Idempotents with small norms. *J. Funct. Anal.*, 270(12):4597–4603, 2016.

[MS20] Nikhil S Mande and Swagato Sanyal. On parity decision trees for Fourier-sparse Boolean functions. *arXiv preprint arXiv:2008.00266*, 2020.

[Neu06] Stefan Neuwirth. Cycles and 1-unconditional matrices. *Proc. London Math. Soc. (3)*, 93(3):761–790, 2006.

[New91] Ilan Newman. Private vs. common random bits in communication complexity. *Inform. Process. Lett.*, 39(2):67–71, 1991.

[Nik06] Vladimir Nikiforov. The smallest eigenvalue of K_r-free graphs. *Discrete Math.*, 306(6):612–616, 2006.

[Nik09] Vladimir Nikiforov. More spectral bounds on the clique and independence numbers. *Journal of Combinatorial Theory, Series B*, 99(6):819–826, 2009.

[Nis91] Noam Nisan. CREW PRAMs and decision trees. *SIAM J. Comput.*, 20(6):999–1007, 1991.

[O'D14] Ryan O'Donnell. *Analysis of Boolean functions*. Cambridge University Press, New York, 2014.

[Pau02] Vern Paulsen. *Completely bounded maps and operator algebras*, volume 78 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2002.

[Pis96] Gilles Pisier. *Similarity problems and completely bounded maps*, volume 1618 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1996.

[Pis12] Gilles Pisier. Grothendieck's theorem, past and present. *Bull. Amer. Math. Soc. (N.S.)*, 49(2):237–323, 2012.

[PR94] Pavel Pudlák and Vojtech Rödl. Some combinatorial-algebraic problems from complexity theory. *Discrete Mathematics*, 1(136):253–279, 1994.

[PSS14] Periklis Papakonstantinou, Dominik Scheder, and Hao Song. Overlays and limited memory communication. In *IEEE 29th Conference on Computational Complexity—CCC 2014*, pages 298–308. IEEE Computer Soc., Los Alamitos, CA, 2014.

[RM97] Ran Raz and Pierre McKenzie. Separation of the monotone NC hierarchy. In *Proceedings 38th Annual Symposium on Foundations of Computer Science*, pages 234–243. IEEE, 1997.

[RS15] Sivaramakrishnan Natarajan Ramamoorthy and Makrand Sinha. On the communication complexity of greater-than. In *2015 53rd Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 442–444. IEEE, 2015.

[RY20] Anup Rao and Amir Yehudayoff. *Communication Complexity: and Applications.* Cambridge University Press, 2020.

[San11] Tom Sanders. A quantitative version of the non-abelian idempotent theorem. *Geom. Funct. Anal.*, 21(1):141–221, 2011.

[San20] Tom Sanders. Bounds in Cohen's idempotent theorem. *J. Fourier Anal. Appl.*, 26(2):Paper No. 25, 64, 2020.

[She11] Alexander A. Sherstov. The pattern matrix method. *SIAM J. Comput.*, 40(6):1969–2000, 2011.

[She14] Alexander A. Sherstov. Communication complexity theory: thirty-five years of set disjointness. In *Mathematical foundations of computer science 2014. Part I*, volume 8634 of *Lecture Notes in Comput. Sci.*, pages 24–43. Springer, Heidelberg, 2014.

[STV17] Amir Shpilka, Avishay Tal, and Ben Lee Volk. On the structure of Boolean functions with small spectral norm. *Comput. Complex.*, 26(1):229–273, March 2017.

[TWXZ13] Hing Yin Tsang, Chung Hoi Wong, Ning Xie, and Shengyu Zhang. Fourier sparsity, spectral norm, and the log-rank conjecture. In *Proceedings of the 2013 IEEE 54th Annual Symposium on Foundations of Computer Science*, FOCS '13, pages 658–667, Washington, DC, USA, 2013. IEEE Computer Society.

[Vio15] Emanuele Viola. The communication complexity of addition. *Combinatorica*, 35(6):703–747, 2015.

[Yao77] Andrew Chi Chih Yao. Probabilistic computations: toward a unified measure of complexity (extended abstract). In *18th Annual Symposium on Foundations of Computer Science (Providence, R.I., 1977)*, pages 222–227. 1977.

[Zha14] Shengyu Zhang. Efficient quantum protocols for XOR-functions. In *Proceedings of the Twenty-fifth Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '14, pages 1878–1885, Philadelphia, PA, USA, 2014. Society for Industrial and Applied Mathematics.

[ZS10] Zhiqiang Zhang and Yaoyun Shi. On the parity complexity measures of Boolean functions. *Theoretical Computer Science*, 411(26-28):2612–2618, 2010.