# Restricted Isometry Constants in Compressed Sensing

*Bubacarr Bah*

Doctor of Philosophy
University of Edinburgh
2012

# Declaration

I declare that this thesis was composed by myself and that the work contained therein is my own, except where explicitly stated otherwise in the text.

(*Bubacarr Bah*)

*To my grandmother, Mama Juma Sowe.*

# Acknowledgement

I wish to express my deepest gratitude to my supervisor, Professor Jared Tanner, for his guidance and support during the course of my PhD. I would follow this with special thanks to my second supervisor, Dr. Coralia Cartis, for her regular monitoring of my progress and her encouragement. Further special thanks to my sponsor the University of Edinburgh through the MTEM Scholarships created in 2007 by the Principal, Professor Sir Timothy O'Shea.

My sincere gratitude goes to Professor Endre Suli of Oxford University who informed me of, and recommended me for, this PhD opening with Professor Jared Tanner and also to my MSc dissertation supervisor, Dr. Radek Erban of Oxford University, for recommending me for this PhD programme.

Many thanks to both the admin and support staff of the School of Mathematics, University of Edinburgh, that contributed to making my PhD programme proceed smoothly. Similar thanks go to members of the Mathematics Teaching Organisation of the school.

I would like to thank the following people for contributing to my research either by responding to a question I posed, discussing an issue pertaining to my research or giving me feedback on my research: Dennis Amelunxen, Jeff Blanchard, Burak Burke, Prof. David Donoho, Martin Lotz, Andrew Thompson, Ke Wei, Pavel Zhlobich. I would also like to thank my officemates not only for the cordial company but for the occasional research related discussions.

I wish to thank members of the Applied and Computational Mathematics research group of the school and members of the Edinburgh Compressed Sensing Reading group. I wish to also thank the first and second set of officials of the Edinburgh SIAM Student Chapter whom I worked with to run the chapter.

Similarly, my thanks go to my friends in Edinburgh that made my stay in the city comfortable and also friends and family in Scotland and England for the moral support.

I would also like to thank the staff of the Institute of Mathematics and its Applications (IMA) at Minnesota who facilitated my visit to the IMA and my Gambian hosts and friends in Minnesota during this visit.

My gratitude goes to my family and to all my friends and well wishers for their unflinching support and encouragement. Above all, special thanks to my parents and wife for the invaluable support.

# Abstract

Compressed Sensing (CS) is a framework where we measure data through a non-adaptive linear mapping with far fewer measurements that the ambient dimension of the data. This is made possible by the exploitation of the inherent structure (simplicity) in the data being measured. The central issues in this framework is the design and analysis of the measurement operator (matrix) and recovery algorithms. Restricted isometry constants (RIC) of the measurement matrix are the most widely used tool for the analysis of CS recovery algorithms. The addition of the subscripts 1 and 2 below reflects the two RIC variants developed in the CS literature, they refer to the $\ell_1$-norm and $\ell_2$-norm respectively.

The RIC$_2$ of a matrix $A$ measures how close to an isometry is the action of $A$ on vectors with few nonzero entries, measured in the $\ell_2$-norm. This, and related quantities, provide a mechanism by which standard eigen-analysis can be applied to topics relying on sparsity. Specifically, the upper and lower RIC$_2$ of a matrix $A$ of size $n \times N$ is the maximum and the minimum deviation from unity (one) of the largest and smallest, respectively, square of singular values of all $\binom{N}{k}$ matrices formed by taking $k$ columns from $A$. Calculation of the RIC$_2$ is intractable for most matrices due to its combinatorial nature; however, many random matrices typically have bounded RIC$_2$ in some range of problem sizes $(k, n, N)$. We provide the best known bound on the RIC$_2$ for Gaussian matrices, which is also the smallest known bound on the RIC$_2$ for any large rectangular matrix. Our results are built on the prior bounds of Blanchard, Cartis, and Tanner in *Compressed Sensing: How sharp is the Restricted Isometry Property?*, with improvements achieved by grouping submatrices that share a substantial number of columns.

RIC$_2$ bounds have been presented for a variety of random matrices, matrix dimensions and sparsity ranges. We provide explicit formulae for RIC$_2$ bounds, of $n \times N$ Gaussian matrices with sparsity $k$, in three settings: a) $n/N$ fixed and $k/n$ approaching zero, b) $k/n$ fixed and $n/N$ approaching zero, and c) $n/N$ approaching zero with $k/n$ decaying inverse logarithmically in $N/n$; in these three settings the RICs a) decay to zero, b) become unbounded (or approach inherent bounds), and c) approach a non-zero constant. Implications of these results for RIC$_2$ based analysis of CS algorithms are presented.

The RIC$_2$ of sparse mean zero random matrices can be bounded by using concentration bounds of Gaussian matrices. However, this RIC$_2$ approach does not capture the benefits of

the sparse matrices, and in so doing gives pessimistic bounds. $\mathrm{RIC}_1$ is a variant of $\mathrm{RIC}_2$ where the nearness to an isometry is measured in the $\ell_1$-norm, which is both able to better capture the structure of sparse matrices and allows for the analysis of non-mean zero matrices.

We consider a probabilistic construction of sparse random matrices where each column has a fixed number of nonzeros whose row indices are drawn uniformly at random. These matrices have a one-to-one correspondence with the adjacency matrices of fixed left degree expander graphs. We present formulae for the expected cardinality of the *set of neighbours* for these graphs, and present a tail bound on the probability that this cardinality will be less than the expected value. Deducible from this bound is a similar bound for the *expansion* of the graph which is of interest in many applications. These bounds are derived through a more detailed analysis of collisions in unions of sets using a *dyadic splitting* technique. This bound allows for quantitative sampling theorems on existence of expander graphs and the sparse random matrices we consider and also quantitative CS sampling theorems when using sparse non mean-zero measurement matrices.

# Contents

# List of Figures

# List of Tables

# Chapter 1

# Introduction

This chapter sets a broader picture by contextualizing this work. In doing so the necessary literature review is covered to show how this work relates to other areas. In Section 1.1 we define restricted isometry constants. Here we showed how RIC$_2$ are related to classical analysis of condition numbers and that sparse non-mean zero matrices have RIC$_1$ instead of RIC$_2$. Consequently, RIC$_2$ led to the discussion on random matrix theory of Gaussian matrices in Section 1.2. A typical example of sparse non-mean zero matrices having RIC$_1$ is the sparse matrices coming from expander graphs, hence the discussion on the random matrix theory of expander graphs in Section 1.3. Compressed sensing being the motivator of this work is then discussed in Section 1.4.

### Notation

The underlying problem of this work is finding a *simple* solution of an underdetermined linear system

$$Ax = y \tag{1.1}$$

where $A \in \mathbb{R}^{n\times N}$, $x \in \mathbb{R}^N$ and $y \in \mathbb{R}^n$ with $n \ll N$. The simple solution sought is a $k$-sparse $x$, i.e., an $x$ with at most $k$ nonzero components. We use the following definition for the $\ell_p$ norm of a vector $z \in \mathbb{R}^N$:

$$\|z\|_p := \begin{cases} \left(\sum_{j=1}^N |z_j|^p\right)^{\frac{1}{p}}, & 0 < p < \infty \\ \max_{j=1,\dots,N} |z_j|, & p = \infty. \end{cases}$$

The $\ell_0$ pseudo-norm, $\|z\|_0$, counts the nonzero entries in $z$. The set of $N$-vectors with at most $k$ nonzero entries is defined as

$$\chi^N(k) := \{z \in \mathbb{R}^N : \|z\|_0 \leq k\}.$$

$A_K$ is the restriction of the columns of $A$ to a support set $K$ with cardinality $k$ ($|K| = k$), and $\lambda^{\max}(B)$ and $\lambda^{\min}(B)$ are the largest and smallest eigenvalues of $B$, respectively. We let $\mathcal{N}(\mu, \sigma^2)$ be the Gaussian distribution with mean $\mu$ and variance $\sigma^2$ and denote the Shannon Entropy with base $e$ logarithms as

$$\mathrm{H}(p) := p \ln\left(\frac{1}{p}\right) + (1-p)\ln\left(\frac{1}{1-p}\right). \tag{1.2}$$

Except stated otherwise, $\Gamma(\cdot)$ represents the gamma function which is defined below both in terms of the factorial function and an improper integral for integers and complex numbers with a positive real part, respectively, [1].

$$\Gamma(n) := (n-1)! \quad \text{and} \quad \Gamma(z) := \int_0^\infty e^{-t} t^{z-1} dt$$

Other notations will be defined when they are first introduced.

## 1.1 Restricted Isometry Constants (RIC)

Many questions in signal processing [11, 74], statistics [5, 53, 94], computer vision [43, 120, 129, 147], and machine learning [30, 42, 98] are employing a parsimonious notion of eigen-analysis to better capture inherent simplicity in the data. This has led to the revisiting of classical eigen-analysis [144, 127] but with a combinatorial twist, which produced a new random matrix theory quantity referred to as sparse principal components [150], sparse eigenvalues [51], or restricted isometry constants (RIC) [39]. In this work we adopt the notation and terminology of RIC.

### 1.1.1 Euclidean Norm Restricted Isometry Constants ($\mathrm{RIC}_2$)

Interest in parsimonious (sparse) solutions to underdetermined systems of equations has seen a rise with the introduction of compressed sensing [59, 39, 38]. The $\ell_2$-norm restricted isometry constant ($\mathrm{RIC}_2$), also referred to as the $\ell_2$-norm restricted isometry property (RIP-2) constant, introduced by Candès and Tao in 2004 [39], is a measure of the greatest relative change that a matrix can induce in the $\ell_2$-norm of sparse vectors. We define the lower and upper $\mathrm{RIC}_2$ of $A$, $L(k,n,N;A)$ and $U(k,n,N;A)$, respectively, in Definition 1.1.1.

**Definition 1.1.1** ([37, 19])**.** *The lower and upper* $\mathrm{RIC}_2$ *of* $A$*,* $L(k,n,N;A)$ *and* $U(k,n,N;A)$*, respectively, are defined as*

$$\begin{aligned} L(k,n,N;A) &:= 1 - \min_{x \in \chi^N(k)} \frac{\|Ax\|_2^2}{\|x\|_2^2}, \\ U(k,n,N;A) &:= \max_{x \in \chi^N(k)} \frac{\|Ax\|_2^2}{\|x\|_2^2} - 1. \end{aligned}$$

Note that, for all expressions involving $L(k,n,N;A)$ it is understood, without explicit statement, that $k$ is limited to the range of values where $L(n,n,N;A) < 1$. Beyond this range of sparsity, there exist $x$ in (1.1) which are mapped to zero, and hence are unrecoverable.

From Definition 1.1.1 we see that RIC$_2$ is related to many established concepts in linear algebra. Firstly, the standard notion of *General Position* is $L(n,n,N;A) < 1$, and *Kruskal rank* [91] is the largest $k$ such that $L(k,n,N;A) < 1$. The RIC$_2$ can be equivalently defined as

$$U(k,n,N;A) := \max_{K\subset\Omega,|K|=k} \lambda^{\max}\left(A_K^* A_K\right) - 1, \tag{1.3}$$

$$L(k,n,N;A) := 1 - \min_{K\subset\Omega,|K|=k} \lambda^{\min}\left(A_K^* A_K\right), \tag{1.4}$$

where $\Omega := \{1,2,\ldots,N\}$. Therefore, the RIC$_2$ $U(k,n,N;A)$ and $L(k,n,N;A)$ measure the maximum and the minimum deviation from unity (one) of the largest and smallest, respectively, square of the singular values of all $\binom{N}{k}$ submatrices of $A$ of size $n \times k$ constructed by taking $k$ columns from $A$. The ratio of the RIC$_2$ $U(k,n,N;A)$ and $L(k,n,N;A)$ is related the $\ell_2$-norm condition number since for each fixed set $K$, the $\ell_2$-norm condition number of $A_K$ is defined as

$$\kappa_2\left(A_K\right) := \sqrt{\frac{\lambda^{\max}\left(A_K^* A_K\right)}{\lambda^{\min}\left(A_K^* A_K\right)}}.$$

Consequently, RIC$_2$ implies a bounded condition number for each $A_K$. As there are $\binom{N}{k}$ of these submatrices, RIC$_2$ analysis is equivalent to classical eigen-analysis with a combinatorial flavour.

RIC$_2$ are defined in terms of the $\ell_2$-norm restricted isometry property (RIP-2) which was introduced by Candès and Tao in [33] as the *uniform uncertainty principle* (UUP) and redefined in terms of RIC and restricted orthogonality constants in [39]. RIP-2 is a sufficient condition on $A$ for exact recovery of a $k$-sparse $x$ in (1.1). Treating the RIC$_2$ as symmetric they expressed the RIP-2 equivalently as follows (note, they used $\delta_k$ instead of $R(k,n,N;A)$).

**Definition 1.1.2** (RIP-2, [33])**.** *An $n \times N$ matrix $A$ has RIP-2, with the smallest* RIC$_2$*, $R(k,n,N;A)$, when the following holds:*

$$\left(1 - R(k,n,N;A)\right)\|x\|_2^2 \le \|Ax\|_2^2 \le \left(1 + R(k,n,N;A)\right)\|x\|_2^2, \quad \forall x \in \chi^N. \tag{1.5}$$

In terms of our definition of RIC$_2$ in Definition 1.1.1 we have

$$R(k,n,N;A) = \max\left(L(k,n,N;A), U(k,n,N;A)\right). \tag{1.6}$$

Formulation (1.5) is referred to as *symmetric* RIC$_2$ while our formulation is referred to *asymmetric*, see [19]. The asymmetric formulation reflects more the behaviour of the extreme eigenvalues as can be seen in Figure 1.1 shown in [19].

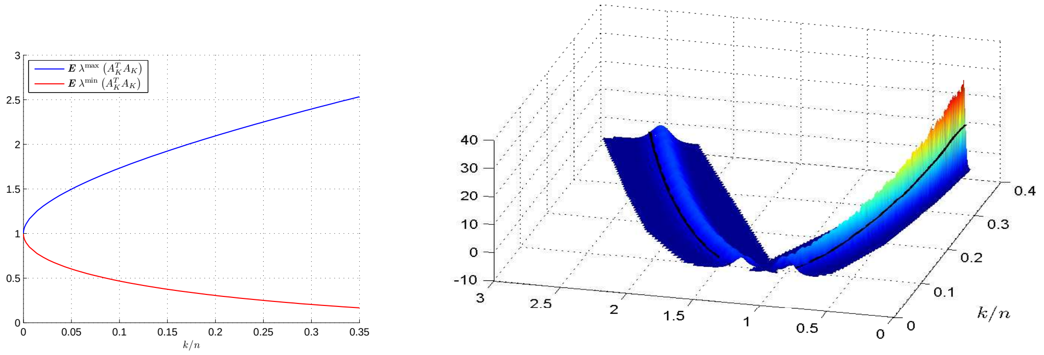

Figure 1.1: *Left panel:* For a given $n \times N$ matrix $A$ and $K \subset [N]$ such that $|K| = k$, the expected values of the largest and smallest eigenvalues of a Wishart matrix $A_K^T A_K$. Note the asymmetry with respect to 1. *Right panel:* **Empirical distributions of the largest and smallest eigenvalues of a Wishart matrix.** "A collection of frequency histograms of $\lambda^{\max}\left(A_K^T A_K\right)$ and $\lambda^{\min}\left(A_K^T A_K\right)$ : x-axis – size of the eigenvalue; y-axis – number of occurrences; z-axis – ratio $k/n$ of the Wishart parameters. Overlays: curves depicting the expected values $\left(1 \pm \sqrt{\rho}\right)^2$ of $\lambda^{\max}\left(A_K^T A_K\right)$ and $\lambda^{\min}\left(A_K^T A_K\right)$, confirming Lemma 1.2.16. Here $n = 200$. At this value of $n$ it is evident that $\lambda^{\max}\left(A_K^T A_K\right)$ and $\lambda^{\min}\left(A_K^T A_K\right)$ lie near, but not on curves. For larger $n$, the concentration would be tighter". *Courtesy of the authors of [19].*

Another important connection worth mentioning is the connection of $\mathrm{RIC}_2$ to the classical study of *Gelfand widths* [86, 69] in approximation theory. With regard to a $k$-sparse solution of the underdetermined system (1.1), if one can choose $A$ it would be helpful to know for what $n$ one is able to get the *optimal reconstruction error.* The optimal reconstruction error is defined as the worst reconstruction error for the *best* $A$ and the *best* method of solving (1.1). Similar problems arise in the area of information-based complexity where one is interested in the recovery of functions $f$ from a class $\mathcal{F}$ by evaluating $n$ functionals applied to $f$ [140]. The optimal error is related to the Gelfand width (also known as $n$-width) of $\mathcal{F}$. A sparse solution to (1.1) is related to the $n$-width of $\ell_1$-balls. In short, Gelfand widths are comparable to quantities that measure the optimal reconstruction error.

In more detail [12, 48, 116], for a given operator (matrix) $A \in \mathbb{R}^{n \times N}$, a normed space $X = \left(\mathbb{R}^N, \|\cdot\|\right)$, and $K \subset X$, the $n$-width is defined as

$$d^n(K, X) := \inf \sup_{x \in K \cap \ker A} \|x\|,$$

where $\ker A := \{z \in \mathbb{R}^N : Az = 0\}$. Let us define the best recovery method as $\triangle : \mathbb{R}^n \to \mathbb{R}^N$ and the maximal reconstruction error by the best possible combination of $A$ and $\triangle$ as

$$E^n(K, X) := \inf \sup_{x \in K} \|x - \triangle(Ax)\|.$$

If the set $K$ is such that $K = -K$ and $K + K \subset C_1 K$ with $C_1 > 0$, then

$$d^n(K, X) \leq E^n(K, X) \leq C_1 d^n(K, X), \quad \text{for} \quad 1 \leq n \leq N. \tag{1.7}$$

Now define the *best k-term approximation* error for a class of vectors $K \subset X$ as

$$\sigma_k(K, X) := \sup_{x \in K} \inf_{z \in \chi^N} \|x - z\|.$$

Let $B_q^N$ be the $\ell_q$ ball in $\mathbb{R}^N$. For $N$-dimensional $\ell_1$ unit balls $K = B_1^N$ and the normed space $X = \ell_2^N := \left(\mathbb{R}^N, \|\cdot\|_2\right)$, Candès and Tao [39] showed that if $A$ has $3R(3k, n, N; A) < 1$ i.e., it has RIP-2 of order $3k$, then we have the following error estimate:

$$\|x - \triangle(Ax)\|_2 \leq \frac{C_2 \sigma_k\left(B_1^N, \ell_2^N\right)}{\sqrt{k}}, \tag{1.8}$$

where $C_2$ only depends on the RIC$_2$, $R(3k, n, N; A)$. The right hand side of (1.8) involves $R(3k, n, N; A)$ while the left hand side is a bound on $E^n\left(B_1^N, \ell_2^N\right)$, and hence a bound on $d^n\left(B_1^N, \ell_2^N\right)$ due to (1.7). This establishes a link between $n$-widths and RIC$_2$, further details can be found in [12, 48, 116].

Moreover, RIP-2 has connection to the *Johnson-Linderstrauss lemma*:

**Lemma 1.1.3** (Johnson-Linderstrauss, [82])**.** *Let $\epsilon \in (0, 1)$ be given. For every set $Q$ of $|Q|$ points in $\mathbb{R}^N$, if $n$ is a positive integer such that $n > n_0 = \mathcal{O}\left(\log\left(|Q|/\epsilon^2\right)\right)$, there exists a Lipschitz mapping $f : \mathbb{R}^N \to \mathbb{R}^n$ such that*

$$(1 - \epsilon)\|u - v\|_2^2 \leq \|f(u) - f(v)\|_2^2 \leq (1 + \epsilon)\|u - v\|_2^2$$

*for all $u, v \in Q$.*

This lemma states that a set of finite point in a high dimensional space can be embedded in a lower dimensional space thereby nearly preserving all mutual distances. This is a consequence of the following concentration inequality [12, 92]:

$$\text{Prob}\left(\left|\|Az\|_2^2 - \|z\|_2^2\right| \geq \epsilon\|z\|_2^2\right) \leq 2e^{-nc_0(\epsilon)}, \quad \epsilon \in (0, 1), \tag{1.9}$$

for any fixed $z \in \mathbb{R}^N$, where the probability is over all $A \in \mathbb{R}^{n \times N}$ and $c_0(\epsilon) > 1$ is a constant that depends only on $\epsilon$. From (1.9) it can be seem that Johnson-Linderstrauss (JL) lemma implies RIP-2. Baraniuk and his co-authors in [12] illustrated that the RIP-2 can be thought of as a straightforward consequence of the JL lemma, and that any distribution that yields a satisfactory JL-embedding will also generate matrices satisfying the RIP-2. Such matrices are referred to as *subgaussian* matrices and they include the centred Gaussian and Bernoulli random matrix ensembles. A definition of these ensembles will be given in Section 1.2.

Unfortunately, due to its combinatorial nature, computing the $\mathrm{RIC}_2$ of a matrix $A$ is in general NP-hard, [108]. To be precise, this is only possible if the problem size $(k, n, N)$ is very small, in which case it is possible to do an exhaustive combinatorial search. As part of a series of efforts in this direction [39, 19], our work in Chapter 2 derived bounds for $\mathrm{RIC}_2$ when the matrices involved are subgaussian. As an extension we derived asymptotic formulae for these bounds in Chapter 3.

### 1.1.2 Manhattan Norm Restricted Isometry Constants $(\mathrm{RIC}_1)$

When the matrices involved are not subgaussian, classical eigen-analysis does not carry through. However, if the matrices are sparse with a fixed number of nonzeros, then a variant of the $\mathrm{RIC}_2$, the $\ell_1$-norm restricted isometry constant $(\mathrm{RIC}_1)$ is used in the analysis. Berinde et al in [15] introduced $\mathrm{RIC}_p$ for $1 \leq p \leq 1 + 1/\log(N)$ but most of the research in this area (including our work) have concentrated on $p = 1$. The lower and upper $\mathrm{RIC}_1$ of $A$, $\overline{L}(k, n, N; A)$ and $\overline{U}(k, n, N; A)$, respectively, are defined as

$$\begin{aligned} \overline{L}(k, n, N; A) &:= 1 - \min_{x \in \chi^N(k)} \frac{\|Ax\|_1}{\|x\|_1} \\ \overline{U}(k, n, N; A) &:= \max_{x \in \chi^N(k)} \frac{\|Ax\|_1}{\|x\|_1} - 1. \end{aligned}$$

Interestingly $\overline{U}(k, n, N; A) = 0$ is trivially achieved for the matrices we consider which are sparse non-mean zero matrices with fixed number of nonzeros per column. This is seen in the format Berinde et al [15] presented the definition of $\mathrm{RIC}_1$ in terms of the $\ell_1$-norm restricted isometry property (RIP-1).

**Definition 1.1.4** (RIP-1)**.** *An $n \times N$ matrix $A$ has RIP-1 when the following condition holds:*

$$\left(1 - \overline{L}(k, n, N; A)\right) ||x||_1 \leq ||Ax||_1 \leq ||x||_1 \quad \forall x \in \chi^N. \tag{1.10}$$

Similar to $\mathrm{RIC}_2$, $\mathrm{RIC}_1$ is a measure of the greatest relative change that a matrix can induce in the $\ell_1$-norm of sparse vectors. This work uses $\mathrm{RIC}_1$ to derive bounds on the probabilistic construction of random matrices with a fixed number of nonzeros per column in Chapter 4, but a brief introductory discussion to this topic is given in Section 1.3.

## 1.2 Random Matrix Theory of Gaussian Matrices

Lacking the ability to calculate the $\mathrm{RIC}_2$ of a given matrix, numerous researchers have developed probabilistic bounds for various random matrix ensembles. As we indicate in [6], these efforts have followed three research programs:

- Determination of the largest ensemble of matrices such that as the problem sizes $(k, n, N)$

grow, the RIC$_2$ $U(k, n, N; A)$ remains bounded above and the $L(k, n, N; A)$ remains bounded away from 1 [103].

- Computing as accurate bounds as possible for particular ensembles, such as the Gaussian ensemble [37, 19], where the entries of $A$ are drawn independent and identically distributed (i.i.d.) from the standard Gaussian $\mathcal{N}(0, 1/n)$. (In part as a model for i.i.d. mean zero ensembles.)

- Computing as accurate bounds as possible for structured random matrices including partial Fourier, Circulant and Toeplitz ensembles [116, 9]. (In part as a model for matrices possessing a fast matrix-vector product.)

This work focuses on the second of these research programs, accurate bounds for the Gaussian ensemble. The motivation to pursue this program is attributed to the existing rich literature on Gaussian random matrices and, with the *universality principle*, the possibility of using the Gaussian ensemble as a model for all mean zero random ensembles.

### 1.2.1 Random Matrix Theory Ensembles

In the field of random matrix theory, there is a wealth of ensembles developed for various application purposes. Here, we would limit ourselves to the description of a few ensembles that have been mentioned or are used in this work. These include selected classical Gaussian and Wishart ensembles, subgaussian random matrices, some of which we use in our eigen-analysis while others we mentioned in the wider compressed sensing discussion coming in Section 1.4; and a few structured random matrices which are also mentioned in the discussion on compressed sensing.

#### Selected Classical Random Matrices

In describing the Gaussian and Wishart matrices we adopt notation used in [64]. In this regard we first define the joint element density of a Gaussian matrix.

**Definition 1.2.1.** *If $A$ is an $n \times N$ Gaussian random matrix $G_\beta(n, N)$, then the joint density of its entries is given by*

$$\frac{1}{(2\pi)^{\beta nN/2}} \exp\left(-\frac{1}{2}\|A\|_F^2\right), \tag{1.11}$$

*where $\beta = 1, 2$ for real or complex, respectively, and $\|A\|_F$ is the Frobenius norm of $A$.*

Instead of the Frobenius norm, the equivalent norm defined by the trace of $A$, trace$(A)$ is also used in the literature. The Frobenius norm, also referred to as the Hilbert Schmidt norm, is defined in various ways, namely,

$$\|A\|_F = \left( \sum_{i=1}^{n} \sum_{j=1}^{N} |a_{ij}|^2 \right)^{\frac{1}{2}} = \left(\text{trace}\,(A^*A)\right)^{\frac{1}{2}} = \left( \sum_{i=1}^{\min(n,N)} \sigma_i^2 \right)^{\frac{1}{2}},$$

where $A^*$ is either $A^T$ or $A^H$ with $A^T$ being the transpose of $A$ and $A^H$, the hermitian (conjugate) transpose of $A$. This norm is invariant to unitary or orthogonal multiplication $\|A\|_F = \|QA\|_F$ for any orthogonal or unitary $Q$ [77]. This gives the so called *orthogonal invariance* or *unitary invariance*, which is a key property of Gaussian ensembles be they real or complex, respectively. The following classical ensembles are constructed from (1.11); as a result they inherit the orthogonal (unitary) invariance property, [64].

- ***Gaussian Orthogonal Ensemble (GOE):*** Let $A = G_1(n,n)$ then a GOE $n \times n$ matrix is formed by $(A + A^T)/2$, hence its symmetric. Its off-diagonal elements are drawn i.i.d. from $\mathcal{N}(0,1/2)$ while its diagonal elements are i.i.d. $\mathcal{N}(0,1)$.

- ***Gaussian Unitary Ensemble (GUE):*** Let $A = G_2(n,n)$ then a GUE $n \times n$ matrix is formed by $(A + A^H)/2$, hence its hermitian. Its off-diagonal elements are drawn i.i.d. from $\mathcal{N}_2(0,1/2)$ while its diagonal elements are i.i.d. $\mathcal{N}(0,1)$.

- ***Wishart Ensemble ($W_\beta(m,n),\ m \geq n$):*** Let $A = G_\beta(m,n)$ then a $W_\beta(m,n)$ is an $n \times n$ matrix formed by $(A^*A)$ where $A^*$ is either $A^T$ or $A^H$, hence its symmetric or hermitian, depending on whether $A$ is real or complex, i.e., $\beta = 1$ or $\beta = 2$ respectively.

### Subgaussian Random Matrices

The class of *subgaussian* random matrices includes the Gaussian ensemble defined above. It is a widely used term in the compressed sensing and sparse approximation literature [103, 104, 116]. We first define what a *subgaussian random variable* is as follows.

**Definition 1.2.2** (Subgaussian Random Variable)**.** *A random variable $X$ is called subgaussian if there exist constants $\beta, \kappa > 0$ (where $\kappa^{-1/2}$ is called the subgaussian moment of $X$) such that*

$$\textit{Prob}\,(|X| \geq t) \leq \beta e^{-\kappa t^2}, \quad \forall t > 0.$$

**Definition 1.2.3** (Subgaussian Ensemble)**.** *An $n \times N$ matrix $A$ is referred to as a subgaussian random matrix if all the entries of $A$ are independent mean zero subgaussian random variables of variances 1, namely, the entries of $A$, $a_{ij}$ for $j \in [n],\ i \in [N]$, satisfy the following.*

$$\textit{Prob}\,(|a_{ij}| \geq t) \leq \beta e^{-\kappa t^2}, \quad \forall t > 0,$$

*where $\beta$ and $\kappa$ are positive constants.*

This implies that the subgaussian ensemble includes the standard Gaussian, the Bernoulli and any matrix whose entries are bounded random variables. If $a_{ij}$ are the entries of an $n \times N$ subgaussian matrix $A$ then prominent examples of the distributions of the $a_{ij}$ include:

$$\textbf{\textit{Gaussian}} \qquad a_{ij} \sim \mathcal{N}\left(0, \frac{1}{n}\right)$$

$$\pm\ \textbf{\textit{Bernoulli}} \qquad a_{ij} := \begin{cases} +\frac{1}{\sqrt{n}} & \text{with probability } \frac{1}{2}, \\ -\frac{1}{\sqrt{n}} & \text{with probability } \frac{1}{2}. \end{cases}$$

$$\textbf{\textit{Other}} \qquad a_{ij} := \begin{cases} +\sqrt{\frac{3}{n}} & \text{with probability } \frac{1}{6}, \\ 0 & \text{with probability } \frac{2}{3}, \\ -\sqrt{\frac{3}{n}} & \text{with probability } \frac{1}{6}. \end{cases}$$

**Structured Random Matrices**

Another class of random matrices of interest are the structured random matrices that admit a Fast Fourier Transform (FFT) implementation and they include the following [116].

- ***Partial Fourier Ensemble (PFE):*** $A$ is an $n \times N$ PFE if it is formed from random rows, $j$, or samples, $t_l$, of a Fourier matrix with entries $F_{j,l} = e^{2\pi i j t_l}$.

- ***Partial Circulant Ensemble (PCE):*** Let $b = (b_0, b_1, \ldots, b_{N-1}) \in \mathbb{C}^N$ and let the matrix $\Phi = \Phi(b) \in \mathbb{C}^{N \times N}$ such that its entries $\phi_{ij} = b_{j-i \mod N}$ for $i, j = 1, \ldots, N$, then $A$ is an $n \times N$ PCE if it is a random draw of $n$ rows of $\Phi$.

- ***Partial Toeplitz Ensemble (PTE):*** Let $b = (b_N, b_{N-1}, \ldots, b_1) \in \mathbb{C}^N$ and let the matrix $\Phi = \Phi(b) \in \mathbb{C}^{N \times N}$ such that its entries $\phi_{ij} = b_{N-j+i}$ for $i, j = 1, \ldots, N$, then $A$ is an $n \times N$ PCE if it is a random draw of $n$ rows of $\Phi$.

### 1.2.2 Extreme Eigenvalues of Gaussian and Wishart Matrices

Focusing on the ensembles of interest here, we discuss the spectrum of Gaussian and Wishart ensembles. We will start by stating briefly what is mainly known about the joint densities of eigenvalues of Gaussian and Wishart matrices. Then we will discuss some asymptotic properties of random matrices implying the so called *universality principle*. We conclude the subsection with a discussion on the largest and smallest eigenvalues of a Wishart matrix.

**Distribution of Eigenvalues**

Recall that RIC$_2$ lower and upper are the deviation from one of the largest and smallest eigenvalues of the Gram matrix formed by a submatrix, $A_K$ of $k$ columns of $A$. In terms of Gaussian matrices we are interested in the squares of the extreme singular values of the Gaussian submatrix $A_K$ which are equivalent to the extreme eigenvalues of the Wishart matrix formed as a Gram matrix from the Gaussian $A_K$. In general for any $n \times m$ Gaussian matrix $G$ and the derived $m \times m$ Wishart matrix $W = G^*G$, the eigenvalues of $W$ will be real due to symmetry irrespective of whether $G$ is from a GOE or a GUE. We will denote and order these eigenvalues as $\lambda_1 \geq \lambda_2 \geq \ldots \lambda_m$. Note that the maximum eigenvalue $\lambda^{\max} = \lambda_1$ while the minimum eigenvalue $\lambda^{\min} = \lambda_m$. In accordance with our previous notation $\lambda^{\max} = \lambda^{\max}(W)$ while $\lambda^{\min} = \lambda^{\min}(W)$. These eigenvalues are the squares of the singular values of $G$ and the $\ell_2$-norm condition number $\kappa_2(G) = \sqrt{\lambda^{\max}/\lambda^{\min}}$. We point out that in the random matrix theory literature, one would find the Wishart matrix formed out of an $n \times m$ Gaussian matrix $G$ to be denoted as an $n \times n$ matrix $W = GG^*$ in which case the spectrum becomes $\lambda^{\max} = \lambda_1 \geq \ldots \lambda_m = \lambda^{\min} \geq 0$, as in [62] and some of the reference therein. However, in either notation the nonzero eigenvalues are the same which is what matters to our analysis.

Using the notation of Edelman and Rao in [64], in Lemma 1.2.4, we state the joint probability density functions (PDF) of the eigenvalues of a given $m \times m$ Wishart (or Laguerre) matrix $W$ and for completeness we will also state, in Lemma 1.2.5, the joint PDF of the eigenvalues of an $n \times n$ Gaussian (or Hermite) random matrix. Main references for these include Dyson (1963) [61], James (1964) [81], Muirhead (1982) [107], Edelman (1989) [63], and Metha (1991) [102].

**Lemma 1.2.4** (Wishart Ensemble [81, 107, 63])**.** *If $\lambda_1 \geq \ldots \geq \lambda_m$ are the eigenvalues of an $m \times m$ Wishart matrix formed from an $n \times m$ Gaussian matrix, then the joint PDF of $\lambda_1, \ldots, \lambda_m$ is*

$$f_\beta(x) = c_L^{\beta,a} \prod_{i<j} |x_i - x_j|^\beta \prod_i x_i^{a-p} \exp\left(-\sum_{i=1}^m x_i^2/2\right)$$

*where $x \in \mathbb{R}^m$ and*

$$c_L^{\beta,a} = \frac{1}{2^{-ma}} \prod_{j=1}^m \frac{\Gamma\left(1 + \frac{\beta}{2}\right)}{\Gamma\left(1 + \frac{\beta}{2}j\right)\Gamma\left(a - \frac{\beta}{2}(m-j)\right)}$$

*for $a = \frac{\beta}{2}n$ and $p = 1 + \frac{\beta}{2}(m-1)$ with $\beta = 1$ and $\beta = 2$ corresponding to the real and complex cases, respectively.*

**Lemma 1.2.5** (Gaussian Ensemble [61, 102])**.** *If $\lambda_1 \geq \ldots \geq \lambda_m$ are the eigenvalues of an $m \times m$ Gaussian random matrix, then the joint PDF of $\lambda_1, \ldots, \lambda_m$ is*

$$f_\beta(x) = c_H^\beta \prod_{i<j} |x_i - x_j|^\beta \exp\left(-\sum_{i=1}^m x_i^2/2\right)$$

*where $x \in \mathbb{R}^m$ and*

$$c_H^\beta = \frac{1}{(2\pi)^{-m/2}} \prod_{j=1}^m \frac{\Gamma\left(1 + \frac{\beta}{2}\right)}{\Gamma\left(1 + \frac{\beta}{2}j\right)}$$

*with $\beta = 1$ and $\beta = 2$ corresponding to the real and complex cases, respectively.*

### The Universality Principle

As mentioned before, the observation that in high dimensions many ensembles have limiting empirical spectral distributions similar to the Gaussian ensemble has been a motivating factor for our work on RIC$_2$ bounds. A great amount of research in random matrix theory has been preoccupied with asymptotic properties of a random ensemble as it dimensions tend to infinity. The analogy of what was expected from such findings is the law of large numbers and the central limit theorem in probability theory [114].

**Lemma 1.2.6** (Law of Large Numbers)**.** *If $X_1, \ldots, X_n$ are $n$ random variables that are i.i.d. with finite variance then $\frac{1}{n}\sum_{i=1}^{n} X_i \to \mu$ as $n \to \infty$ where $\mu$ is the population mean.*

**Lemma 1.2.7** (Central Limit Theorem)**.** *If $X_1, \ldots, X_n$ are $n$ random variables that are i.i.d. with finite variance, $\sigma^2$, then as $n \to \infty$ the distribution of the normalized deviation*

$$\frac{1}{\sqrt{n}}\left(\sum_{i=1}^{n} X_i - n\mu\right) \to \mathcal{N}\left(0, \sigma^2\right).$$

Clearly what matters in the above two examples is the mean and the variance but not the distribution the $X_i$ are drawn from. Such asymptotic behaviour is referred to as the *invariance principle* and something similar has been observed about the distributions of eigenvalues of random matrices in the high-dimensional limit. An example of this phenomenon is *Wigner's semicircle law* proved by Wigner [146] in the 1950s.

**Lemma 1.2.8** (Wigner's Semicircle Law)**.** *If an $n \times n$ random matrix $A$ is a GOE or a GUE, then the normalised eigenvalues $\frac{\lambda_1}{\sqrt{n}}, \ldots, \frac{\lambda_n}{\sqrt{n}}$ are asymptotically distributed according to the semicircular distribution, $F$, with density*

$$f(x) = \begin{cases} \frac{1}{2\pi}\sqrt{4 - x^2} & |x| \leq 2, \\ 0 & |x| > 2. \end{cases}$$

Another example of this phenomenon is the *Marchenko-Pastur quarter-circle law* [99] governing the limiting distribution of the spectrum of a Wishart matrix.

**Lemma 1.2.9** (Marchenko-Pastur Quarter-circle Law)**.** *If $W$ is an $m \times m$ Wishart matrix formed from an $n \times m$ Gaussian random matrix and $m/n \to \rho \in (0,1)$ as $(m,n) \to \infty$, then the normalised eigenvalues $\frac{\lambda_1}{n}, \ldots, \frac{\lambda_n}{n}$ are asymptotically distributed according to the distribution, $F$, with density*

$$f(x) = \begin{cases} \frac{1}{2\pi x \rho}\sqrt{(b - x)(x - a)} & [a, b], \\ 0 & \textit{otherwise}, \end{cases}$$

*where $a = \left(1 - \sqrt{\rho}\right)^2$ and $b = \left(1 + \sqrt{\rho}\right)^2$.*

This is also referred to as the *Quarter-circle law* in which case it is reformulated to be about the singular values of a normalized Gaussian matrix. There is also the celebrated *Girko's circular law* [71] also referred to as the *Circular conjecture* on the limiting distribution of the spectrum of non Gaussian random matrices. This law states that under some reasonable conditions the eigenvalues of an $n \times n$ random matrix with independent entries having mean 0 and variance $1/n$ fall uniformly on a circular disk of radius 1 as $n \to \infty$. There is a well-known intuition behind these theorems and conjectures, the *universality* phenomenon, that asserts that the limiting distribution should not depend on the particular distribution of the entries. This universality phenomenon has been observed numerically for many decades. More recently, rigorous explanations of this phenomenon have been found, see the work of Tao and Vu [137, 136] and the references therein.

### Distribution of Extreme Eigenvalues

Ever since the seminal paper on condition numbers by von Neumann and Goldstine [144], it is well known in computational mathematics (numerical analysis) that the condition number of a matrix plays a crucial role in the computation of solutions of linear systems and the computation of eigenvalues. For instance, condition numbers have been used in the quest to understand the numerical accuracy of Gaussian Elimination which was first worked on by Trefethen and Schreiber [142]. Precisely, condition numbers are key in determining the convergence and stability of a numerical algorithm. Random matrices are often used as *test matrices* for algorithms and hence the use of random eigenvalues was introduced by von Neumann and Goldstine [144] to further understand the behaviour of condition numbers. This is one reason for having a lot of remarkable results in the random matrix literature about the extreme eigenvalues of Wishart matrices. The other two main applications that are part of the driving force of the field are nuclear physics and multivariate statistics. Note that Wishart matrices are equivalent to covariance matrices in multivariate statistics.

Estimates of the smallest $\lambda^{\min}$ and largest $\lambda^{\max}$ eigenvalues of a Wishart are given by Silverstein in [125] and Geman in [70], respectively. Furthermore, in certain cases we know the exact distribution of these extreme eigenvalues in terms of zonal polynomials or hypergeometric functions of matrix arguments, see [90, 130]; but these exact distributions are almost impossible to compute. Fortunately, simpler bounds have also been derived by Edelman [63]. In addition to being simpler to compute, bounds on the PDF of $\lambda^{\min}$ and $\lambda^{\max}$ have been used in the derivation of bounds on the tails of condition number distributions. Below is a statement of some of these results in the real cases, for the complex cases the reader is referred to the references above.

Theorem 1.2.10 gives an exact distribution of $\lambda^{\min}$. Despite the fact that the PDF of $\lambda^{\min}$ given in this theorem is computable, the limiting distribution as $n \to \infty$ of $n\lambda^{\min}$, which is much simpler is given in Corollary 1.2.11. We then give a bound on the PDF of $\lambda^{\min}$ and $\lambda^{\max}$ in Lemmas 1.2.12 and 1.2.13, respectively, their proofs can be found in [62, 46].

**Theorem 1.2.10** (Smallest Eigenvalue [90])**.** *If $W$ is an $n \times n$ Wishart matrix with $n \geq 1$, then the PDF of $\lambda^{\min}$ is given by*

$$f_{\lambda^{\min}}(x) = \frac{n}{2^{n-1/2}} \cdot \frac{\Gamma(n)}{\Gamma(n/2)} \cdot x^{-1/2} \cdot e^{-xn/2} \cdot U\left(\frac{n-1}{2}, \frac{1}{2}, \frac{x}{2}\right).$$

*When $a > 0$ and $b < 1$, the Tricomi function, $U(a, b, z)$, is the unique solution to the Kummer's equation*

$$z\frac{d^2w}{dz^2} + (b - z)\frac{dw}{dz} - aw = 0$$

*satisfying $U(a, b, 0) = \Gamma(1 - b)/\Gamma(1 + a - b)$ and $U(a, b, \infty) = 0$.*

**Corollary 1.2.11** ([62])**.** *If $W$ is an $n \times n$ Wishart matrix with $n \geq 1$, then as $n \to \infty$, $n\lambda^{\min}$ converges in distribution to a random variable whose PDF is given by*

$$f(x) = \frac{1 + \sqrt{x}}{2\sqrt{x}} \cdot e^{-(x/2+\sqrt{x})}$$

**Lemma 1.2.12** ([62])**.** *If $W$ has the distribution of an $n \times n$ Wishart matrix derived from an $m \times n$ Gaussian matrix, then the PDF of $\lambda^{\min}$, $f_{\lambda^{\min}}(x)$, satisfies*

$$f_{\lambda^{\min}}(x) \leq \frac{\pi^{1/2} \cdot 2^{(n-m+1)/2}\Gamma\left(\frac{n+1}{2}\right)}{\Gamma\left(\frac{m}{2}\right)\Gamma\left(\frac{n-m+1}{2}\right)\Gamma\left(\frac{n-m+2}{2}\right)} \cdot x^{(n-m-1)/2} \cdot e^{-x/2}.$$

**Lemma 1.2.13** ([62])**.** *If $W$ has the distribution of an $n \times n$ Wishart matrix derived from an $m \times n$ Gaussian matrix, then the PDF of $\lambda^{\max}$, $f_{\lambda^{\max}}(x)$, satisfies*

$$f_{\lambda^{\max}}(x) \leq \frac{\pi^{1/2} \cdot 2^{(1-n-m)/2}}{\Gamma(n/2)\Gamma(m/2)} \cdot x^{(n+m-3)/2} \cdot e^{-x/2}.$$

The convergence of $\lambda^{\max}$ also depends on the limit of the ratio of the number of rows to the number of columns of the rectangular Gaussian matrix used to form the Wishart matrix. The ratio must be bounded as the dimension of the matrix goes to infinity. In the next lemma we state the *almost sure convergence* of $\lambda^{\min}$ and $\lambda^{\max}$ due to Silverstein [125] and Geman [70], respectively. Initially this lemma was stated in [62] with *convergence in probability.*

**Definition 1.2.14** ([114])**.** *A sequence of random variables $(X_n : n = 1, 2, 3, \ldots)$ is said to converge to a random variable $X$ almost surely (a.s.) if Prob$(X_n \to X) = 1$ as $n \to \infty$.*

**Definition 1.2.15** ([114])**.** *A sequence of random variables $(X_n : n = 1, 2, 3, \ldots)$ is said to converge to a random variable $X$ in probability if Prob$(|X_n - X| \geq \epsilon) = 0$ as $n \to \infty$ for all $\epsilon > 0$.*

**Lemma 1.2.16** ([62])**.** *If $W$ is an $n \times n$ Wishart matrix derived from an $m \times n$ Gaussian matrix, with $\lim_{n\to\infty} m/n = \rho$, then*

$$\begin{aligned} (1/n)\,\lambda^{\min} &\overset{a.s.}{\longrightarrow} (1-\sqrt{\rho})^2 \quad \textit{for} \quad 0 \leq \rho < 1 \\ (1/n)\,\lambda^{\max} &\overset{a.s.}{\longrightarrow} (1+\sqrt{\rho})^2 \quad \textit{for} \quad 0 \leq \rho \leq \infty. \end{aligned}$$

Using the above results on the smallest and largest eigenvalues of Wishart matrices, one can derive bounds on the tails distribution of upper and lower RIC$_2$ $L(k,n,N;A)$ and $U(k,n,N;A)$, respectively, for a given $n\times N$ Gaussian matrix, $A$, as was classically done for condition numbers. Remember that the Gramian matrix of a submatrix $A_K$ is a $k \times k$ Wishart matrix. In fact, the bounds provided by Lemmas 1.2.12 and 1.2.13 were particularly useful in the derivation of sharper RIC$_2$ bounds in Chapter 2; while we confirm the asymptotic limits prescribed by Lemma 1.2.16 in the asymptotic formulae we derive for the RIC$_2$ bounds in Chapter 3.

## 1.3 Sparse Random Matrices and Expander Graphs

Going back to the underlying underdetermined system (1.1), the parsimonious solution usually sought after exploits the inherent structure (sparsity) in the data, $x$. Then if the sparsity of the vector is $k$, there is strong motivation to make the number of rows of the matrix in the underdetermined system, $n$, to be as close to $k$ as possible, *optimal* $n$, which is when $n = \mathcal{O}(k)$. This will be defined more precisely when we discuss compressed sensing, as an example of an application where this work is useful, in Section 1.4. The significance of the RIC$_2$ analysis is that it gives sufficient recovery guarantees for matrices that have small RIC$_2$ with optimal $n$. It is now well known that subgaussain matrices have this property but these matrices are dense and therefore have computational bottlenecks.

On the other hand, sparse matrices are particularly appealing to applied and computational mathematics (numerical analysis) communities because of their low storage complexity and the existence of very fast implementation routines compared to dense matrices; [77, 54, 141] are just a few references in a large and growing list. This is why efforts were made to use sparse matrices in compressed sensing and sparse approximation. Of late, significant progress has been made in this direction with papers such as [149, 15, 16, 80] giving both theoretical performance guarantees and also exhibiting numerical results that show sparse matrices coming from expander graphs to be as good sensing matrices as their dense counterparts. In fact, Blanchard and Tanner [21] recently demonstrated in a GPU implementation how well these type of matrices do compared to dense Gaussian and Discrete Cosine Transform matrices even with very small fixed number of nonzeros per column.

Now we discuss the graphs that underlie these matrices – expander graphs. Expander graphs were first defined by Bassalygo and Pinsker [13], and their existence first proved by Pinsker in the early 70s [112]. Expander graphs due to their many uses can be defined in at least three different ways. *Combinatorially* an expander graph is a highly connected graph for which you need to remove a high percentage of its edges in order to disconnect it. *Geometrically* every set of vertices in an expander graph has a very large boundary - isoperimetry. *Probabilistically* an expander graph is such that a random walk on its vertices very rapidly converges to its limiting distribution. *Algebraically* an expander graph has the first positive eigenvalue of its Laplace operator bounded away from zero. A more quantitative definition of a lossless expander graph is given in Definition 1.3.1 and its diagrammatic illustration in Figure 1.2.

**Definition 1.3.1** ([41])**.** *$G = (U, V, E)$ is a lossless $(k, d, \epsilon)$-expander if it is a bipartite graph with a set of left vertices $U$, set of right vertices $V$ and set of edges $E$ where $|U| = N$ and $|V| = n$ and has a regular left degree $d$, such that any $X \subset U$ with $|X| \leq k$ has $|\Gamma(X)| \geq (1-\epsilon)\, d|X|$ neighbours.* [1]

**Remark 1.3.2.**

1. *These expander graphs are* lossless *because $\epsilon \ll 1$;*
2. *They are referred to as* unbalanced expanders *when $n \ll N$;*
3. *The* expansion *of a lossless $(k, d, \epsilon)$-expander graph is $(1-\epsilon)\, d$;*
4. *Regular left degree $d$ means that all vertices in $U$ have the same degree $d$.*

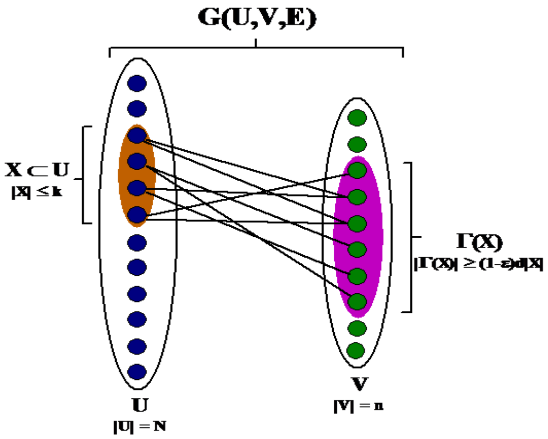

Figure 1.2: An illustration of a lossless $(k, d, \epsilon)$-expander graph with $k = 4$ and $d = 2$.

Simply put, Definition 1.3.1 means that almost all neighbours of a small subset of left vertices, $X \subset U$, are *unique neighbours*, i.e., each vertex in $\Gamma(X)$ has degree 1 into $X$. In other words, small enough left vertex sets have almost the maximal expansion. Note that for this to be possible we must have $k \leq n/d$ and the best expansion one can hope for is $k = n/d$. Typically we are interested in minimising the left degree $d$ and maximising the expansion factor.

Based on the area and the application for which they are studied, the study of expander graphs has been either about structural issues, deterministic construction issues, algorithmic

[1] *Lossless expanders* with parameters $d, k, n, N$ are equivalent to *lossless conductors* with parameters that are base 2 logarithms of the parameters of *lossless expanders* see [76, 15] and the references therein.

issues or the issues of their expansion in relation to similar concepts in other disciplines. For details on any of the above-mentioned issues see the review article by Hoory, Linial and Wigderson [76]. For applications that this work is focussed on, the concern is about the explicit construction of these graphs. Pinsker [112] proved their existence and showed that any left-regular bipartite graph, whose vertices are generated uniformly at random, is with high probability an expander graph. Precisely, a non-constructive probabilistic argument shows that lossless expander graphs do exist with optimal parameters $d, n$ as stated in the proposition below.

**Proposition 1.3.3** (Probabilistic Construction, [41]). *For any $N/2 \geq k \geq 1,~ \epsilon > 0$ there exists a lossless $(k,d,\epsilon)$-expander with*

$$d = \mathcal{O}\left(\log\left(N/k\right)/\epsilon\right) \quad \textit{and} \quad n = \mathcal{O}\left(k\log\left(N/k\right)/\epsilon^2\right).$$

Unfortunately, deterministic constructions only achieve sub-optimal parameters. It is well known in the graph theory community that the second largest eigenvalue of a graph serves as a good measure of its expansion [2, 3, 135]. The best explicit construction of expander graph using the second largest eigenvalue was obtained using Ramanujan graphs which have optimal second largest eigenvalue [95]. However this only achieved expansion $d/2$, even for the case $n = N$. To get expansion beyond $d/2$, necessary to obtain lossless expanders, an alternative method has to be invented since Kahale proved in [85] that some Ramanujan graphs do not expand more than $d/2$. Using alternative methods weaker objects similar to lossless expanders and lossless expanders with weaker parameters were constructed, see [115, 117, 132]. The first alternative construction for lossless expanders was due to Capalbo [40] but it was only for the balanced case ($n = N$). Capalbo's construction used high min-entropy extractors derived in [119] and graph products. Later, Capalbo et al in [41] achieved a significant and more general results that is an extension of both the constructions of [40] and [119]. Their technique involves a zig-zag product of conductors and their result is stated in the theorem below.

**Theorem 1.3.4** (Theorem 1, [80]). *Let $0 < r < 1$ be a fixed constant. Then for large enough $n$ there exists a $\left(\alpha n, d, \frac{1}{4}\right)$-expander graph $G$ with $n$ variable nodes and $\frac{n}{r}$ parity check nodes for some $0 < \alpha < 1$ with constant left degree or sub-linearly growing with $n$. Furthermore, the explicit zig-zag construction can deterministically construct the expander graph.*

The best explicit construction (though sub-optimal) so far is credited to Guruswami et al [72]. Their construction used Parvaresh-Vardy codes [110] and is stated in the theorem below.

**Theorem 1.3.5** (Theorem 7, [80]). *For any constant $\alpha > 0$, and any $N, k, \epsilon > 0$, there exist a $(k,d,\epsilon)$-expander graph with left degree and number of right side vertices as*

$$d = \mathcal{O}\left(\left(\log(N)/\epsilon\right)^{1+1/\alpha}\right) \quad \textit{and} \quad n = \mathcal{O}\left(d^2k^{1+\alpha}\right).$$

Expander graphs have been well studied in theoretical computer science and pure mathematics but their uses spans beyond these two areas. Due to their expansion property they have *computational* uses in communication networks and coding theory; *mathematical* uses in metric embeddings; *statistical* uses in Markov Chains; and *physical* uses in Monte-Carlo algorithms in statistical mechanics. We will briefly describe a few common uses of expander graphs, for further insight see [41] or [76] for a more detailed survey.

1. **Distributed Routing in Networks:** Certain applications, see [111, 4, 26], desire networks having pairs of nodes connected via vertex or edge disjoint paths such that these paths can be found efficiently and in a parallel way even if requests for connections arrive on-line. If we take the network to be a lossless expander then a constant fraction of the input nodes in $X$ will send messages to their direct neighbours. This way, this constant fraction of $|X|$ nodes can disconnect from $X$ after matching up with a unique neighbour. The process is continued iteratively and it should conclude in $\mathcal{O}\left(\log\left(|X|\right)\right)$ steps instead of being pipelined as would happen in a general algorithm.

2. **Linear Time Decodable Error-Correcting Codes:** In the context of Low Density Parity Check (LDPC) codes it has been shown ([96, 126, 128] and references therein) that lossless expanders can be used to yield asymptotically good linear codes of constant rate with a linear-time decoding algorithm that makes $\mathcal{O}\left(\log\left(N\right)\right)$ parallel steps. Again if $G$ is a lossless expander, the rate will be $1 - n/N$ and for constant $d$ this can be arbitrarily close to 1.

3. **Bitprobe Complexity of Storing Subsets:** This is about storing $k$-subset of $[N]$ in binary vectors of length $n$. Based on a scheme proposed by the authors of [28] in which you query only one bit of the vector in order to determine its membership to $[N]$, lossless expander were used to achieve optimal construction of smallest $n$ for constant error.

For application to compressed sensing and sparse approximation the problem is that the adjacency matrices of expander graphs do not have small RIC$_2$ with optimal $n$. Chandar showed in [44] that such sparse *binary* matrices need $n = \Omega(k^2)$ to have small enough RIC$_2$. This is where RIC$_1$ comes into play. It provides guarantees of optimal $n$ when the matrix has small RIC$_1$.

Given that we do not have an optimal explicit construction for expander graphs, sampling theorems about when a random bipartite graph is, with high probability, a lossless expander might be useful to the practitioner. Consequently, such sampling theorems will be about the generation of random binary matrices that approximate, with high probability, adjacency matrices of lossless expander graphs. Chapter 4 provides a bound on the tail of the distribution of the size of expansion using a novel technique of *dyadic splitting of sets*, and from this tail bound, derives the aforementioned sampling theorems.

## 1.4 Motivating Example – Compressed Sensing

Our work on RIC was motivated by compressed sensing although it has applications wider than compressed sensing. In this section we give a brief introduction to compressed sensing, mainly to put thing into perspective. We start by a non-quantitative general description of compressed sensing and we follow this up in Section 1.4.1 with a mathematical formulation of the compressed sensing problems and the typical mathematical issues that arise. We conclude with a list of selected applications of compressed sensing in Section 1.4.2.

In recent times, there has been a data deluge and traditional ways of handling this data needed to be improved upon. The need for more efficient handling of high dimensional data sets coming from information systems and signal processing led to the emergence of compressed sensing or compressive sampling, seminal papers include [39, 38, 59]. In fact, the birth of compressed sensing could be attributed to the following question posed by David Donoho, who is credited with coining the word *compressed sensing*.

> "Since most of the information in the signal is contained in only a few coefficients and the rest of the signal is not needed for the applications, can one directly determine (acquire) only the relevant coefficients without reading (measuring) each of the coefficients?" [59]

The answer is *yes* provided there is some underling simplicity in the signal (data) and the measurement process is done linearly with an appropriate measurement matrix. In essence, compressed sensing is measuring information at the *information rate*, as oppose to doing measurements (sampling) at the so called Shannon-Nyquist rate (for a signal) [124] which is equivalent to taking as many measurements as the dimension of the signal.

The underlying simplicity in the vector of interest is usually *sparsity* or *compressibility.* By sparsity we mean the vector through a basis transformation has a coefficient vector that has relatively few nonzero entries when compared to the dimension of the vector itself. If the vector is sparse in the canonical basis then the coefficient vector corresponds to the vector itself. On the other hand, a vector is compressible if after a basis transformation its coefficients vector have few large (in magnitude) components with the majority of the entries having magnitude zero or close to zero. Interestingly, there is a very large class of signals (vectors) that are either sparse or compressible and compressed sensing could be applied for this class of signals.

The ability to take few measurements in compressed sensing has both time and cost implications in the measurement process. The fundamental change in the processing system is the shift of burden to computing resources, this would become clearer when we discuss algorithms in Section 1.4.1. Assuming there is not too much sacrifice in quality, it turns out that this shift is beneficial both in terms of time and real cost. This is why wherever the conditions for the application of compressed sensing exist we see rise in its use. In Section 1.4.2 we state some real life applications of compressed sensing.

Although new, compressed sensing is related to other established disciplines and recently the compressed sensing concept has been extended to other areas. We would mention some of these links and for any further details the interested reader is referred to the references provided. Compressed sensing is considered part of sparse approximation [27] with roots in signal processing, harmonic analysis [58] and numerical analysis [47]. As a result there has been as wide range of techniques and algorithms common to both compressed sensing and other areas of sparse approximation. It is also significant to note that there has been an overlap in terms of analysis techniques between compressed sensing and approximation theory. The connection of RIC$_2$ to $n$-widths or RIP-2 to the Johnson-Linderstrauss lemma mentioned earlier is a case in point [12, 89]. It is also worth mentioning that, particularly in the algorithms for compressed sensing, convex optimization tools have been used extensively and this will become evident throughout the thesis starting from Section 1.4.1. Of late, there have been extensions of ideas from compressed sensing to a closely related area called Matrix Completion [31, 118]. For a detailed introduction to compressed sensing see the following papers [10, 39, 36, 59, 27].

### 1.4.1 Mathematics of Compressed Sensing

Let $x \in \mathbb{R}^N$ be the vector (signal) of interest. Instead of directly measuring $x$ we *sense* $x$ by taking linear projections of $x$, i.e., we take measurements of $x$ that are inner product of $x$ with other vectors, say $a_i$. The outcome is a measurement vector $y \in \mathbb{R}^n$ where $y_i = \langle a_i, x \rangle$. The dimension of the measurement vector is far smaller than the ambient dimension of $x$ since $n \ll N$ and this is where the gain in the time of the measurement process is registered. Stacking the vectors $a_i$ into rows of a matrix gives an $n \times N$ *measurement* or *sensing* matrix $A$ and the whole sensing process leads to the underdetermined linear system (1.1). Simply put, we sense $x$ by applying a matrix $A$ to it to get $y$. If we fix $A$ in advance the measurement process is referred to as *non-adaptive* while if $A$ is modified during the process then we have an *adaptive* one.

Now with $A$ and $y$ we try to recover $x$ which is equivalent to solving the underdetermined system (1.1), $y = Ax$. Getting a unique solution is the challenge but with the inherent simplicity of $x$ we can exactly recover $x$ or recover a very good approximation of $x$. If $x$ is $k-$sparse in some basis then $x = B\alpha$ where $B$ is a basis matrix and $\alpha$ is a coefficient vector having only $k$ nonzero entries. Without loss of generality assume $B = I$ where $I$ is the identity matrix then we look for the sparsest $x$ that satisfies our system $y = Ax$ as

$$\min_{x \in \chi^N} \|x\|_0 \quad \text{subject to} \quad Ax = y. \tag{1.12}$$

If on the other hand, $x$ is compressible or we want to cater for noise in the measurement process we consider this modified linear system

$$y = Ax + e \tag{1.13}$$

where $e$ is a noise vector capturing the model misfit or the non-sparsity (compressibility) of the signal $x$. So the $\ell_0$-minimization problem (1.12) in the noise case becomes

$$\min_{x \in \chi^N} \|x\|_0 \quad \text{subject to} \quad \|Ax - y\|_2 < \|e\|_2, \tag{1.14}$$

where $\|e\|_2$ is the magnitude of the noise. If $B \neq I$, we have $Ax = AB\alpha$ in which case we let $Z = AB$ and replace $Ax$ by $Z\alpha$ in problems (1.14) and (1.12) above. Consequently, the solution derived has to be appropriately transformed to get $x$.

By now it is should be apparent that the main mathematical problem in compressed sensing is the design of a sensing matrix, $A$ and algorithms to solve (1.14) and (1.12). Sensing matrices and algorithms are also referred to as encoders and decoders, respectively. The pair are supposed to be interdependent but it is surprising that we can design an encoder separate from the decoder and also that we can design algorithms independent of the measurement matrix used. It is in this regard that we will discuss these two issues separately.

### Sensing Matrices

The main purpose of compressed sensing is to take few measurements, $n$, far less than the signal dimension, $N$. Ideally, we would like to design matrices with $n = k$ rows but this is not possible in practice except if we have some *magical* way of knowing where the nonzeros of $x$ are in advance. Generally matrices with optimal recovery guarantees can be designed both deterministically and probabilistically with $n = \Omega(k^2)$ rows [55, 49]. What this means is that we can either have an explicit or probabilistic construction of a measurement matrix with $n = \Omega(k^2)$ rows and we can give guarantees that any algorithm can be used to recover $x$. This bound on the number of measurements is derived using *coherence* which, like RIC, is another tool of analysis in compressed sensing. The coherence measure, $\mu$, of a matrix $A$ with $\ell_2$ normalised columns $a_i$ is defined as

$$\mu = \max_{i \neq j} |\langle a_i, a_j \rangle| \,.$$

This bound on $n$ is very pessimistic since $k^2$ can be very large and we might end up taking close to $N$ measurements diminishing the whole point of doing compressed sensing.

The good news is if we use $\text{RIC}_2$ instead of coherence we can have $n = \mathcal{O}(k)$ with a small order constant for certain ensembles (originally proven by [39, 59]). To be precise we take measurements

$$n \geq Ck \log^{\alpha}(N/k) \quad \text{for} \quad C > 0 \quad \text{and} \quad \alpha \geq 1, \tag{1.15}$$

where $C$ is a universal constant independent of the problem instance, $(k, n, N)$. This is a remarkable achievement in compressed sensing because up to a log-factor the number of measurements scale linearly in the sparsity, $k$, instead of quadratic as we sated earlier while the dimension of the signal is only felt in the log-factor. We point out that not all matrices have this optimal order of number of measurements. Specifically, all attempts to design a deterministic $A$ with optimal reconstruction guarantees have failed to produce provably optimal $n$. Some explicit constructions using tight frames are close but fall short of the optimal [65, 45]. Interestingly, the breakthrough was made possible via random matrices. Ensembles including mean zero subgaussian matrices [12] and some structured random matrices like Fourier, Toeplitz and Circulant matrices [116, 73] achieve this optimal $n$ with $\alpha = 1$ and $\alpha = 5$, respectively.

Unfortunately, sparse non-mean zero matrices do not have RIP-2 for $n = \mathcal{O}(k)$, in fact, as earlier mentioned, Chandar [44] showed that *binary* matrices with $\{0, 1\}$ entries only have bounded RIC$_2$ if the number of measurements, $n = \Omega(k^2)$. However, by having small enough RIC$_1$ binary matrices that are adjacency matrices of lossless expander graphs also attained the optimal $n$ in (1.15) with $\alpha = 1$ [15]. Our work in Chapter 4 extends these optimal guarantees to adjacency matrices of lossless expander graphs with random sign on the nonzeros.

### Algorithms

Compressed sensing algorithms generally fall into two categories: optimization and greedy algorithms. The former relaxes the problems (1.12) and (1.14) into a convex or non-convex optimization problem and then uses existing optimization methods to get an approximate solution; while the latter tackles the combinatorial problems (1.12) and (1.14) directly, attempting to identify the right support set through a greedy search.

**Optimization Algorithms:** The term *optimization algorithms* is misnomer because these are actually methods for which there exists a host of algorithms. Optimization methods relax the $\ell_0$-minimization problem (1.12), similarly for (1.14), into an $\ell_q$-minimization for $0 < q \leq 1$

$$\min_{x \in \chi^N} \|x\|_q \quad \text{subject to} \quad Ax = y. \tag{1.16}$$

We use this regime for $q$ as the $\ell_q$ norms are sparsifying norms. For $0 < q < 1$ the problem becomes non-convex and solving it might be as hard as the original $\ell_0$ problem. However, we have a convex relaxation of (1.12) if $q = 1$ and (1.16) becomes the following convex problem commonly known as *$\ell_1$-minimization or basis pursuit*,

$$\min_{x \in \chi^N} \|x\|_1 \quad \text{subject to} \quad Ax = y. \tag{1.17}$$

The $\ell_1$ relaxation of (1.14) gives the *quadratically constrained basis pursuit* also referred as *basis pursuit denoising*. This can be solved with efficient methods from convex optimization and analysis for $\ell_1$ recovery guarantees abound, pioneering work include [39, 59] for dense $A$ or [15] for sparse matrices. To give an idea about the type of guarantees we refer to we state and prove a simple example in the form of Theorem 1.4.1 whose original proof is found in [116, 66].

**Theorem 1.4.1.** *If the* $\mathrm{RIC}_2$ *of order* $2k$, $L(2k, n, N; A)$ *and* $U(2k, n, N; A)$, *of an* $n \times N$ *matrix,* $A$, *satisfies*

$$\max\left(L(2k, n, N; A), U(2k, n, N; A)\right) < 1/3, \tag{1.18}$$

*then every* $k$*-sparse vector* $x \in \mathbb{R}^N$ *is recovered by* $\ell_1$*-minimization.*

The proof of Theorem 1.4.1 makes use of the *null space property* (NSP) which, similar to $\mathrm{RIC}_2$, is another tool of analysis in compressed sensing particularly for $\ell_1$-minimization.

**Definition 1.4.2** (NSP)**.** *An* $n \times N$ *matrix,* $A$ *satisfies the null space property of order* $k$ *if for all* $K \subset \Omega$ *with* $\Omega = \{1, \ldots, N\}$ *and* $|K| = k$ *the following holds*

$$\|v_K\|_1 < \|v_{\overline{K}}\|_1 \quad \forall v \in \ker A \setminus \emptyset \tag{1.19}$$

*where* $\overline{K} = \Omega \setminus K$ *and* $v_K$ *is* $v$ *except for indices not in* $K$ *for which it has zero entries.*

Theorem 1.4.3 gives a recovery guaranty for $\ell_1$-minimization based on the null space property, see [116, 66] for it's proof.

**Theorem 1.4.3.** *For an* $n \times N$ *matrix* $A$, *every* $k$*-sparse vector* $x \in \mathbb{R}^N$ *is the unique minimizer of* (1.17) *if and only if* $A$ *satisfies the null space property.*

*Proof.* So to prove Theorem 1.4.1 it suffice to so that for $v \in \ker A \setminus \emptyset$, (1.18) implies (1.19) and we proceed to show this as thus. Let $v \in \ker A \setminus \emptyset$, $K_0$ be the set of the largest in magnitude $k$ entries of $v$, $K_1 \in \overline{K_0}$ be the second set of the largest in magnitude $k$ entries of $v$, $K_2 \in \overline{K_0 \cup K_1}$ be the third set of the largest in magnitude $k$ entries of $v$, and so on.

Now let $R(k, n, N; A) = \max\left(L(k, n, N; A), U(k, n, N; A)\right)$ and we use $R_k$ as a shorthand for $R(k, n, N; A)$. Using the lower bound of the RIP-2 in (1.5) we have

$$\begin{aligned}
\|v_{K_0}\|_2^2 &\leq \frac{1}{1 - R_k}\|Av_{K_0}\|_2^2 && (1.20)\\
&= \frac{1}{1 - R_k}\langle Av_{K_0}, (-Av_{K_1} - Av_{K_2} - Av_{K_3} - \cdots)\rangle && (1.21)\\
&\leq \frac{1}{1 - R_{2k}}\sum_{j \geq 1}\langle Av_{K_0}, -Av_{K_j}\rangle && (1.22)\\
&\leq \frac{R_{2k}}{1 - R_{2k}}\|v_{K_0}\|_2 \sum_{j \geq 1}\|v_{K_j}\|_2. && (1.23)
\end{aligned}$$

From (1.20) to (1.21) we use the fact that if $v \in \ker A \setminus \emptyset$ then $Av_{K_0} = -Av_{K_1} - Av_{K_2} - Av_{K_3} - \cdots$. From (1.21) to (1.22) we use the property that the RIC$_2$ is non-decreasing in the first argument i.e., $R_s \leq R_{2s} \leq R_{3s} \leq \ldots$ which is a consequence of the spectrum of a Wishart matrix. From (1.22) to (1.23) we use the property that $\langle Av_{K_0}, -Av_{K_j} \rangle \leq R_{2k} \|v_{K_0}\|_2 \|v_{K_j}\|_2$ which follows from using Hölder's inequality and the definition of $R_k$. Now, dividing (1.23) by $\|v_{K_0}\|_2$ yields

$$\|v_{K_0}\|_2 \leq \frac{R_{2k}}{1 - R_{2k}} \sum_{j \geq 1} \|v_{K_j}\|_2. \tag{1.24}$$

By our ordering of the $v_{K_j}$ we know that for $j \geq 1$, the $k$ entries of $v_{K_j}$ are bounded from above by the $k$ entries of $v_{K_{j-1}}$ which implies that $\|v_{K_j}\|_2 \leq \|v_{K_{j-1}}\|_2$. Using the equivalence of norms we have $\|v_{K_{j-1}}\|_2 \leq \frac{1}{\sqrt{k}} \|v_{K_{j-1}}\|_1$ and hence $\|v_{K_j}\|_2 \leq \frac{1}{\sqrt{k}} \|v_{K_{j-1}}\|_1$. We substitute this in (1.24) to have

$$\|v_{K_0}\|_2 \leq \frac{R_{2k}}{\sqrt{k}\,(1 - R_{2k})} \sum_{j \geq 1} \|v_{K_{j-1}}\|_1 \tag{1.25}$$

$$\sqrt{k}\|v_{K_0}\|_2 \leq \frac{R_{2k}}{1 - R_{2k}} \left( \|v_{K_0}\|_1 + \|v_{\overline{K}_0}\|_1 \right) \tag{1.26}$$

$$\|v_{K_0}\|_1 \leq \frac{1}{2} \left( \|v_{K_0}\|_1 + \|v_{\overline{K}_0}\|_1 \right). \tag{1.27}$$

From (1.25) to (1.26) we moved the $\sqrt{k}$ to the left hand side and rewrite $\sum_{j \geq 1} \|v_{K_{j-1}}\|_1$ as $\|v_{K_0}\|_1 + \|v_{\overline{K}_0}\|_1$. From (1.26) to (1.27) we again use the equivalence of norms to bound from below the left hand side and use (1.18) to upper bound the right hand side. Inequality (1.27) gives the null space property (1.21) and it holds if (1.18) holds, hence concluding the proof. □

Further discussion on recovery guarantees for $\ell_1$-minimization will be done when discussing sampling theorems and phase transitions for compressed sensing algorithms in Chapter 2 for the dense matrices and Chapter 4 for the sparse matrices.

**Greedy Algorithms:** There are many specifically designed *greedy* algorithms for the $\ell_0$ problems (1.12) and (1.14). Many greedy algorithms have been designed for dense sensing matrices [27] and several others for sparse matrices [15]. We will just list the ones relevant to this work: Orthogonal Matching Pursuit (OMP) popularized by [143], for a more general setting see [138], Iterative Hard Thresholding (IHT), [25], now improved to Normalised Iterative Hard Thresholding (NIHT), [24], Compressive Sampling Matching Pursuits (CoSaMP), [109], and Subspace Pursuit (SP), [50]. A more detailed discussion of these algorithms and their recovery guarantees will be given in Chapter 2.

When $A$ is sparse and non-mean zero, a different set of greedy algorithms have been proposed. They include Expander Matching Pursuit (EMP), [78], Sparse Matching Pursuit

(SMP), [18], Sequential Sparse Matching Pursuit (SSMP), [17], Left Degree Dependent Signal Recovery (LDDSR), [148], and Expander Recovery (ER), [79, 80]. A more detailed discussion of these other set of algorithms and their recovery guarantees will be given in Chapter 4.

### 1.4.2 Applications of Compressed Sensing

The range of applications where compressed sensing can be applied is wide, as a results the ones we mention here are by no means an exhaustive list. We also give references where more details about a given application can be found: Single-Pixel Camera, see [133, 10], Magnetic Resonance Imaging (MRI), see [97], Radar and Sonar, see [75], Error Correction, see [39, 57, 121], Statistics and Machine Learning, see [34, 139, 122, 113], Low-Rank Matrix Recovery, see [31, 35, 118].

## 1.5 Conclusion

**Summary of Chapter**

This thesis addresses restricted isometry constants (RIC) which are random matrix quantities whose use has spiked with the introduction of compressed sensing. The $\ell_p$-norm RIC determines how close to an isometry a matrix $A$ is when applied to vectors $x$, for $p = 1, 2$. The analysis of RIC$_2$ is related to classical eigen-analysis of condition numbers, the only difference being the combinatorial nature of RIC$_2$. It is known that, for dense matrices, only random matrices has bounded RIC$_2$ of optimal order of number of rows of $A$, $n = \mathcal{O}(k)$. Subgaussian matrices have the smallest order constant that is a product of an absolute constant and a factor logarithmic in the dimension of $x$, $N$. Sparse non-mean zero matrices need to have bounded RIC$_1$ to attain the optimal order for $n$. For this reason after the introduction of RIC$_2$ and RIC$_1$, there was a discussion on Gaussian matrices in Section 1.2 and sparse matrices from expander graphs in Section 1.3.

In the discussion on Gaussian random matrices other ensembles that were relevant to this work were introduced and spectral properties of Gaussian and their composite, Wishart, matrices were also discussed. Due to the relationship between the extreme eigenvalues and RIC$_2$, the distribution of the extreme values of Wishart matrices and their asymptotic properties were revisited. Sparse matrices were mentioned in the context of binary matrices with fixed nonzeros per column. These are adjacency matrices of lossless expander graphs, hence the exposition on expander graph.

Given that this whole research in this area was motivated from compressed sensing. Section 1.4 was devoted to a review of compressed sensing, mainly stressing on the mathematics that arise from the compressed sensing problem and giving a picture of how this ties up with the RIC analysis. The mathematical issues that arise in compressed sensing is the design and analysis of sensing matrices and recovery algorithms. A brief discussion on this was followed by a listing of applications of compressed sensing.

### Contributions of Thesis

The contributions of the work include the following:

- The derivation of the smallest known bounds on RIC$_2$ for Gaussian random matrices.
- Using a novel technique of grouping submatrices with significant column overlap and hence reducing the combinatorial term from the union bound of the $\binom{N}{k}$ submatrices.
- The use of a probabilistic method to come up with a covering argument that enables us to quantify the sufficient number of groups to cover at the $\binom{N}{k}$ submatrices.
- The derivation of formulae for the RIC$_2$ bounds of Gaussian random matrices in three different asymptotic regimes of $(k, n, N)$. The case where the ratio $n/N$ is fixed and the ratio $k/n$ goes to zero; the case where the ratio $k/n$ is fixed and the ratio $n/N$ goes to zero; and the case where both ratios $n/N$ and $k/n$ go to zero but the latter going to zero at a rate inverse logarithmic in the reciprocal of the former along a path $\gamma$.
- The derivation of limit functions that the RIC$_2$ converge to in terms of $\gamma$ only.
- The derivation of a tail bound on the number of rows with at least one nonzero of binary matrices with a fixed number of nonzeros per column. Equivalently, this is a tail bound on the size of the set of neighbours and the expansion of lossless expander graphs.
- The use of a novel technique of dyadic splitting of sets to derive this tail bound.
- The use of this tail bound combined with RIC$_1$ to derive of quantitative sampling theorem for when a random draw of a binary matrix with fixed number of nonzeros approximates with high probability the matrices we consider; or for when a random draw of a bipartite graph becomes a lossless expander with high probability.
- The derivation of sampling theorems for compressed sensing algorithms using such sparse non-mean zero matrices and the use of these sampling theorems to compare performance guarantees of these algorithms using the phase transition framework.

### Outline of Thesis

**Chapter Two** is on the derivation of bounds on RIC$_2$ for Gaussian random matrices. The first bounds were derived by Candès and Tao (CT) using concentration of measure inequalities for extreme singular values of Gaussian matrices and a union bound over the $\binom{N}{k}$ submatrices. The CT bounds were improved upon by Blanchard, Cartis and Tanner (BCT) using more accurate probability density functions (PDF) of extreme eigenvalues of Wishart matrices and a union bound too. This work made significant improvement over the BCT by using a novel technique of grouping submatrices with significant column overlap and hence reducing the combinatorial from the union bound. The validity of our bounds for finite problem sizes and their implications for compressed sensing are also presented.

**Chapter Three** is on the derivation of formulae for the $\mathrm{RIC}_2$ bounds of Gaussian random matrices. This was done in three different asymptotic regimes of the problem size $(k, n, N)$. The case where the ratio $n/N$ is fixed and the ratio $k/n$ goes to zero; the case where the ratio $k/n$ is fixed and the ratio $n/N$ goes to zero; and the case where both ratios $n/N$ and $k/n$ go to zero but the latter going to zero inverse logarithmically in the reciprocal of the former along a path $\gamma$. From the third case we derived limit functions that the $\mathrm{RIC}_2$ converge to in terms of $\gamma$ only. These asymptotic approximations of the bounds provided sampling theorems consistent with compressed sensing literature.

**Chapter Four** is on the derivation of a tail bound on the number of rows with at least one nonzero of binary matrices with fixed number of nonzeros per column. Equivalently, this is a tail bound on the size of the set of neighbours and the expansion of lossless expander graphs. We use a technique of dyadic splitting of sets to derive this tail bound. Moreover, using the above tail bound combined with $\mathrm{RIC}_1$, we derived a quantitative sampling theorem for when a random draw of a binary matrix with fixed nonzero approximates, with high probability, the matrices we consider. In other words, we provide a sampling theorem for when a random draw of a bipartite graph becomes, with high probability, a lossless expander. Finally, we present sampling theorems for compressed sensing algorithms using such sparse non-mean zero matrices and we used this to compare performance guarantees of these algorithms using the phase transition framework. We also compared performance guarantees of $\ell_1$-minimization for when the matrix is dense versus when the matrix is sparse.

**Conclusion** summaries the main points of the thesis and suggested possible extensions of the work in the thesis.

# Chapter 2

# Extreme Eigenvalues of Gaussian Submatrices

## 2.1 Introduction

We have established the link between extreme eigenvalues of Gaussian submatrices and the $\ell_2$-norm restricted isometry constants (RIC$_2$) in Chapter 1. Again in Chapter 1 we argued that many of the theorems in compressed sensing rely upon a *sensing matrix* having suitable bounds on its RIC$_2$ and this is also true generally for any parsimonious solution of the underdetermined linear system (1.1). Unfortunately, computing the RIC$_2$ of a matrix $A$ is in general NP-hard, [108]. Efforts are underway to design algorithms that compute accurate bounds on the RIC$_2$ of a matrix [52, 84], but to date these algorithms have a limited success, with the bounds only effective for $k = \Omega\left(n^{1/2}\right)$.

In this chapter we focus on the derivation of accurate bounds for the Gaussian ensemble. Candès and Tao derived the first set of RIC$_2$ bounds for the Gaussian ensemble using a union bound over all $\binom{N}{k}$ submatrices and bounding the singular values of each submatrix using concentration of measure bounds [39]. Blanchard, Cartis and Tanner derived the second set of RIC$_2$ bounds for the Gaussian ensemble, similarly using a union bound over all $\binom{N}{k}$ submatrices, but achieved substantial improvements by using more accurate bounds on the probability density function of Wishart matrices [19]. These bounds are presented here in Theorem 2.2.2 and Theorem 2.2.4 respectively. This work presents yet further improved bounds for the Gaussian ensemble, see Theorem 2.3.2 and Figure 2.3, by grouping submatrices with overlapping support sets, say, $A_K$ and $A_{K'}$ with $|K \cap K'| \gg 1$, for which we expect the singular values to be highly correlated. These are the first RIC$_2$ bounds that exploit this structure. In addition to asymptotic bounds for large problem sizes, we present bounds valid for finite values of $(k, n, N)$.

The Chapter [1] is organised as follows: Prior asymptotic bounds are presented in Section 2.2. Our improved bounds and their comparison with those in Theorem 2.2.4 is given in Section 2.3 and the derivation is described in Section 2.3.1. The bounds' validity for finite values is demonstrated in Section 2.4 and the implications of the $\mathrm{RIC}_2$ bounds for compressed sensing is given in Section 2.5. Proof of technical lemmas used or assumed in our discussion come in the Section 2.6.

We focus our attention on bounding the $\mathrm{RIC}_2$ for the Gaussian ensemble in the setting of *proportional-growth asymptotics*, also referred to as the *linear-growth asymptotics*, defined below.

**Definition 2.1.1** (Proportional-Growth Asymptotics)**.** *A sequence of problem sizes* $(k, n, N)$ *is said to follow proportional-growth asymptotics if*

$$\frac{k}{n} = \rho_n \to \rho \quad \text{and} \quad \frac{n}{N} = \delta_n \to \delta \quad \text{for} \quad (\delta, \rho) \in (0,1)^2 \quad \text{as} \quad (k, n, N) \to \infty. \tag{2.1}$$

In this asymptotic setting, we provide quantitative values above which it is exponentially unlikely that the $\mathrm{RIC}_2$ will exceed. In Section 2.4 we show how our derivation of these bounds can also supply probabilities for specified bounds and finite values of $(k, n, N)$.

We point out that in [123] the authors came up with lower bounds for $\mathrm{RIC}_2$ of any matrix seemingly better than the bounds we present here for Gaussian matrices. However, they only showed that one of these bounds is valid for $k = 2$. This may be due to a low dimensional effect and the bound is likely to grow substantially for larger values of $k$. There is literature that supports this claim. In [65], Elad developed an algorithm that constructs matrices with good $\mathrm{RIC}_2$, and they show big improvement for small $k$. However, when the problem size grows this algorithm looses the gain over what one gets from a random Gaussian. The other bound in [123] is beyond the useful range of the $\mathrm{RIC}_2$.

## 2.2 Prior $\mathrm{RIC}_2$ Bounds

### CT $\mathrm{RIC}_2$ bounds:

There have been two previous quantitative bounds for the $\mathrm{RIC}_2$ of the Gaussian ensemble in the proportional-growth asymptotics. The first bounds on the $\mathrm{RIC}_2$ of the Gaussian ensemble were supplied in [39] by Candès and Tao using union bounds and concentration of measure bounds on the extreme eigenvalues of Wishart matrices from [92, 131]. With notation adjusted to match the notation used in the bounds we derived, these bounds are stated in Theorem 2.2.2 with Definition 2.2.1 defining some of the terms used in the theorem, and plots of these bounds are displayed in Figure 2.1.

[1] Material in this chapter is published in [6] in a joint authorship with J. Tanner whose permission has been obtained for the inclusion of the material.

**Definition 2.2.1.** *Let* $(\delta,\rho)\in(0,1)^2$ *and* $H(\cdot)$ *be the Shannon Entropy function with base* $e$ *logarithms given in* (1.2)*. Define*

$$\mathcal{U}^{CT}(\delta,\rho) := \left[1+\sqrt{\rho}+(2\delta^{-1}H(\delta\rho))^{1/2}\right]^2-1$$

*and*

$$\mathcal{L}^{CT}(\delta,\rho) := 1-\max\left\{0,\left[1-\sqrt{\rho}-(2\delta^{-1}H(\delta\rho))^{1/2}\right]^2\right\}.$$

**Theorem 2.2.2** (Candès and Tao [39])**.** *Let $A$ be a matrix of size $n\times N$ whose entries are drawn i.i.d. from $\mathcal{N}(0,1/n)$. Let $\delta$ and $\rho$ be defined as in* (2.1)*, and $\mathcal{L}^{CT}(\delta,\rho)$ and $\mathcal{U}^{CT}(\delta,\rho)$ be defined as in Definition 2.2.1. For any fixed $\epsilon>0$, in the proportional-growth asymptotics,*

$$Prob(L(k,n,N;A)<\mathcal{L}^{CT}(\delta,\rho)+\epsilon)\to 1 \quad and \quad Prob(U(k,n,N;A)<\mathcal{U}^{CT}(\delta,\rho)+\epsilon)\to 1$$

*exponentially in $n$.*

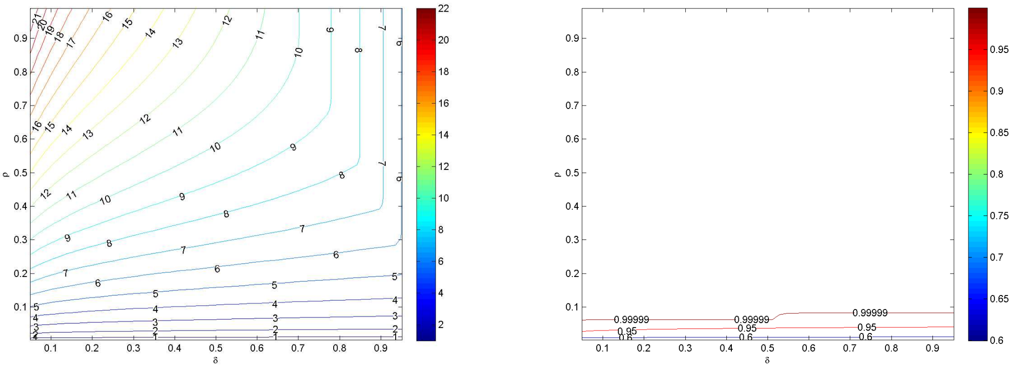

Figure 2.1: The RIC$_2$ bounds from Definition 2.2.1 for $(\delta,\rho)\in(0,1)^2$; *left panel:* $\mathcal{U}^{CT}(\delta,\rho)$ and *right panel:* $\mathcal{L}^{CT}(\delta,\rho)$.

### BCT RIC$_2$ Bounds

Our bounds follow the construction of the second bounds on the RIC$_2$ for the Gaussian ensemble, presented in [19] by Blanchard, Cartis and Tanner. These bounds are stated in Theorem 2.2.4 with Definition 2.2.3 defining some of the terms used in the theorem, and plots of these bounds are displayed in Figure 2.2.

**Definition 2.2.3.** *Let* $(\delta,\rho)\in(0,1)^2$ *and define*

$$\psi_{\min}(\lambda,\rho) := H(\rho)+\frac{1}{2}\Big[(1-\rho)\ln\lambda+\rho\ln\rho+1-\rho-\lambda\Big], \tag{2.2}$$

$$\psi_{\max}(\lambda,\rho) := \frac{1}{2}\Big[(1+\rho)\ln\lambda-\rho\ln\rho+1+\rho-\lambda\Big]. \tag{2.3}$$

*Define* $\lambda^{\min}_{BCT}(\delta,\rho)$ *and* $\lambda^{\max}_{BCT}(\delta,\rho)$ *as the solution to* (2.4) *and* (2.5) *respectively:*

$$\delta\psi_{\min}\left(\lambda^{\min}_{BCT}(\delta,\rho),\rho\right) + H(\rho\delta) = 0, \quad \textit{for} \quad \lambda^{\min}_{BCT}(\delta,\rho) \le 1-\rho, \tag{2.4}$$

$$\delta\psi_{\max}\left(\lambda^{\max}_{BCT}(\delta,\rho),\rho\right) + H(\rho\delta) = 0, \quad \textit{for} \quad \lambda^{\max}_{BCT}(\delta,\rho) \ge 1+\rho. \tag{2.5}$$

*Define*

$$\mathcal{L}^{BCT}(\delta,\rho) := 1 - \lambda^{\min}_{BCT}(\delta,\rho) \quad \textit{and} \quad \mathcal{U}^{BCT}(\delta,\rho) := \min_{\nu\in[\rho,1]} \lambda^{\max}_{BCT}(\delta,\nu) - 1. \tag{2.6}$$

**Theorem 2.2.4** (Blanchard, Cartis, and Tanner [19])**.** *Let $A$ be a matrix of size $n \times N$ whose entries are drawn i.i.d. from $\mathcal{N}(0,1/n)$. Let $\delta$ and $\rho$ be defined as in* (2.1)*, and $\mathcal{L}^{BCT}(\delta,\rho)$ and $\mathcal{U}^{BCT}(\delta,\rho)$ be defined as in Definition 2.2.3. For any fixed $\epsilon > 0$, in the proportional-growth asymptotics,*

$$\textit{Prob}(L(k,n,N;A) < \mathcal{L}^{BCT}(\delta,\rho)+\epsilon) \to 1 \quad \textit{and} \quad \textit{Prob}(U(k,n,N;A) < \mathcal{U}^{BCT}(\delta,\rho)+\epsilon) \to 1$$

*exponentially in $n$.*

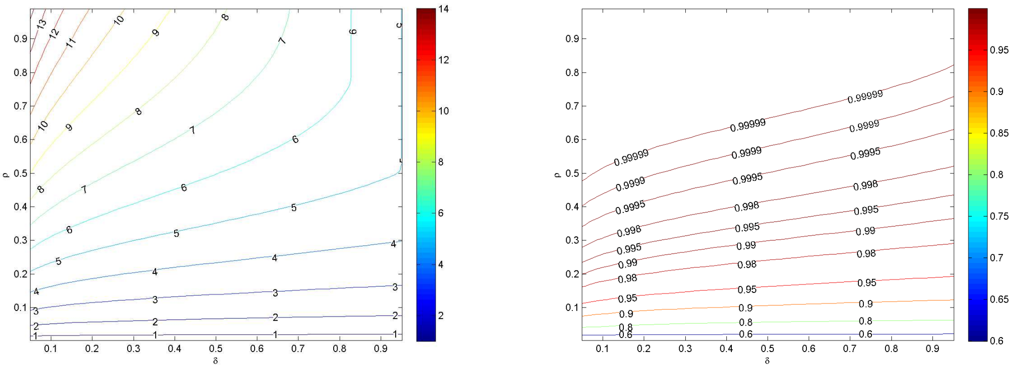

Figure 2.2: The $\text{RIC}_2$ bounds from Definition 2.2.3 for $(\delta,\rho)\in(0,1)^2$; *left panel:* $\mathcal{U}^{BCT}(\delta,\rho)$ and *right panel:* $\mathcal{L}^{BCT}(\delta,\rho)$.

Figures 2.1 and 2.2 show that the bounds in Theorem 2.2.4 are a substantial improvement on those in Theorem 2.2.2.

## 2.3 Improved $\text{RIC}_2$ Bounds

The probability density functions (PDF's) of the $\text{RIC}_2$ for the Gaussian ensemble is currently unknown, but asymptotic probabilistic bounds have been proven. Our bounds, and earlier ones, for the $\text{RIC}_2$ of the Gaussian ensemble are built upon bounds on the PDF's of the extreme eigenvalues of Wishart matrices due to Edelman [64, 62]. All earlier bounds on the $\text{RIC}_2$

have been derived using union bounds that consider each of the $\binom{N}{k}$ submatrices of size $n \times k$ individually [19, 39]. We consider groups of submatrices where the columns of the submatrices in a group are from at most $m \geq k$ distinct columns of $A$. We present our improved bounds in Theorem 2.3.2, preceded by the definition of the terms used in it given in Definition 2.3.1. Plots of these bounds are displayed in Figure 2.3.

**Definition 2.3.1.** *Let* $(\delta, \rho) \in (0,1)^2$ *and* $\gamma \in [\rho, \delta^{-1}]$. *Let* $\psi_{\min}(\lambda, \gamma)$ *and* $\psi_{\max}(\lambda, \gamma)$ *be defined as in* (2.2) *and* (2.3), *respectively. Define* $\lambda^{\min}(\delta, \rho; \gamma)$ *and* $\lambda^{\max}(\delta, \rho; \gamma)$ *as the solution to* (2.7) *and* (2.8) *respectively:*

$$\delta\psi_{\min}\left(\lambda^{\min}(\delta,\rho;\gamma),\gamma\right) + H(\rho\delta) - \delta\gamma H(\rho/\gamma) = 0, \quad \textit{for } \lambda^{\min}(\delta,\rho;\gamma) \leq 1-\gamma, \tag{2.7}$$

$$\delta\psi_{\max}\left(\lambda^{\max}(\delta,\rho;\gamma),\gamma\right) + H(\rho\delta) - \delta\gamma H(\rho/\gamma) = 0, \quad \textit{for } \lambda^{\max}(\delta,\rho;\gamma) \geq 1+\gamma. \tag{2.8}$$

*Let* $\lambda^{\min}_{BT}(\delta,\rho) := \max_{\gamma} \lambda^{\min}(\delta,\rho;\gamma)$ *and* $\lambda^{\max}_{BT}(\delta,\rho) := \min_{\gamma} \lambda^{\max}(\delta,\rho;\gamma)$ *and define*

$$\mathcal{L}^{BT}(\delta,\rho) := 1 - \lambda^{\min}_{BT}(\delta,\rho) \quad \textit{and} \quad \mathcal{U}^{BT}(\delta,\rho) := \lambda^{\max}_{BT}(\delta,\rho) - 1. \tag{2.9}$$

That for each $(\delta, \rho; \gamma)$, (2.7) and (2.8) have a unique solution $\lambda^{\min}(\delta, \rho; \gamma)$ and $\lambda^{\max}(\delta, \rho; \gamma)$ respectively was proven in [19]. That $\lambda^{\min}(\delta, \rho; \gamma)$ and $\lambda^{\max}(\delta, \rho; \gamma)$ have unique maxima and minima respectively over $\gamma \in [\rho, \delta^{-1}]$ is established in Lemma 2.3.5.

**Theorem 2.3.2.** *Let* $A$ *be a matrix of size* $n \times N$ *whose entries are drawn i.i.d. from* $\mathcal{N}(0, 1/n)$. *Let* $\delta$ *and* $\rho$ *be defined as in* (2.1), *and* $\mathcal{L}^{BT}(\delta,\rho)$ *and* $\mathcal{U}^{BT}(\delta,\rho)$ *be defined as in Definition 2.3.1. For any fixed* $\epsilon > 0$, *in the proportional-growth asymptotics,*

$$\textit{Prob}(L(k,n,N;A) < \mathcal{L}^{BT}(\delta,\rho) + \epsilon) \to 1 \quad \textit{and} \quad \textit{Prob}(U(k,n,N;A) < \mathcal{U}^{BT}(\delta,\rho) + \epsilon) \to 1$$

*exponentially in* $n$.

In the spirit of reproducible research, software and web forms that evaluate $\mathcal{L}^{BT}(\delta, \rho)$ and $\mathcal{U}^{BT}(\delta, \rho)$ are publicly available at [100].

### Comparison of Improved Bounds to Empirical Lower Bounds

Sharpness of the bounds can be probed by comparison with empirically observed lower bounds on the RIC$_2$ for finite-dimensional draws from the Gaussian ensemble. There exist efficient algorithms for calculating lower bounds of RIC$_2$ [60, 83]. These algorithms perform local searches for submatrices with extremal eigenvalues. The new bounds in Theorem 2.3.2, see Figure 2.3, can be compared with empirical data displayed in Figure 2.4.

To further demonstrate the sharpness of our bounds, we compute the maximum and minimum "sharpness ratios" of the bounds in Theorem 2.3.2 to empirically observed lower bounds;

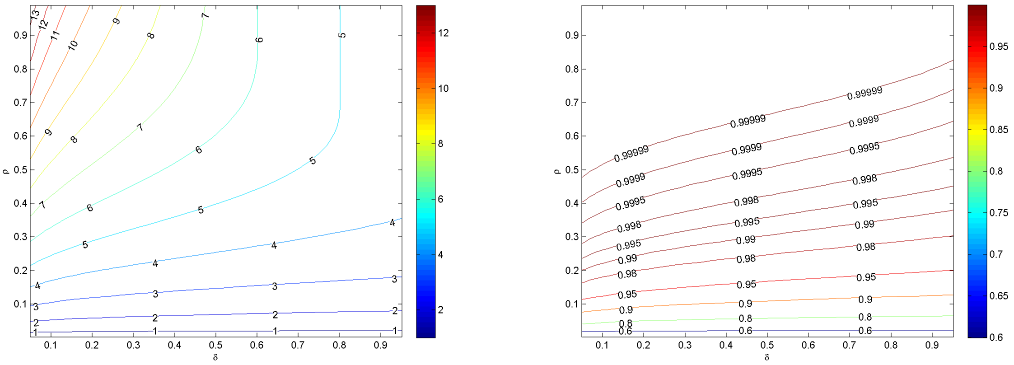

Figure 2.3: The $\mathrm{RIC}_2$ bounds from Definition 2.3.1 for $(\delta,\rho)\in(0,1)^2$; *left panel:* $\mathcal{U}^{BT}(\delta,\rho)$ and *right panel:* $\mathcal{L}^{BT}(\delta,\rho)$.

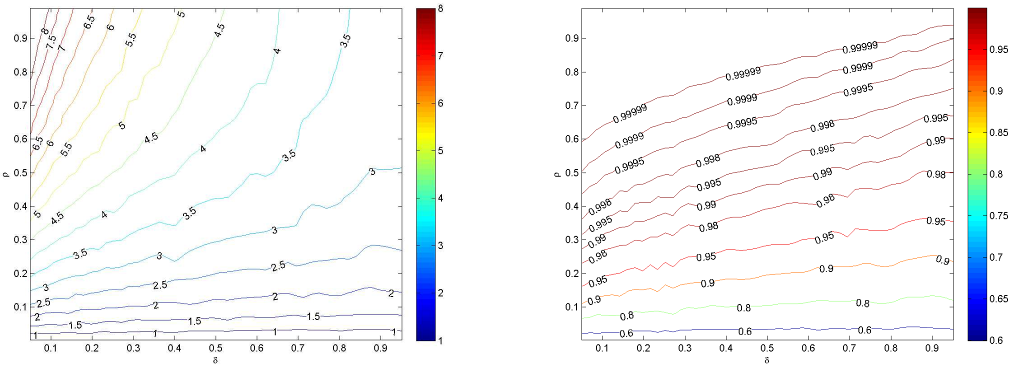

Figure 2.4: **Empirically observed lower bounds on** $\mathrm{RIC}_2$ **for** $A$ **Gaussian.** Observed lower bounds of *left panel:* $L(k,n,N;A)$ and *right panel:* $U(k,n,N;A)$. Although there is no computationally tractable method for calculating the $\mathrm{RIC}_2$ of a matrix, there are efficient algorithms that perform local searches for extremal eigenvalues of submatrices, allowing for observable lower bounds on the $\mathrm{RIC}_2$. Algorithm for observing $L(k,n,N;A)$ [60] and $U(k,n,N;A)$ [83] were applied to hundreds of $A$ drawn i.i.d. $\mathcal{N}(0,1/n)$ with $n=400$ and $N$ increasing from 420 to 8000.

for each $\rho$, the maximum and minimum of the ratio is taken over all $\delta\in[0.05,0.9524]$. These are the same $\delta$ values used in Figure 2.4. These ratios are shown in the left panel of Figure 2.5, and are below 1.57 of the empirically observed lower bounds on $L(k,n,N;A)$ and $U(k,n,N;A)$ computed with $n=400$.

### Comparison of Improved Bounds to Prior Bounds

Since the BCT bounds are a significant improvement of the CT bounds, it suffice to show how ours compare to the BCT bounds. The bounds presented here in Definition 2.3.1 and Theorem 2.3.2 are a further improvement over those in [19], as stated in Corollary 2.3.6 deducible from Lemma 2.3.5. The right panel of Figure 2.5 shows the ratio of the previously best known bounds, Theorem 2.2.4, to the new bounds, Theorem 2.3.2; for each $\rho$, the ratio is maximized

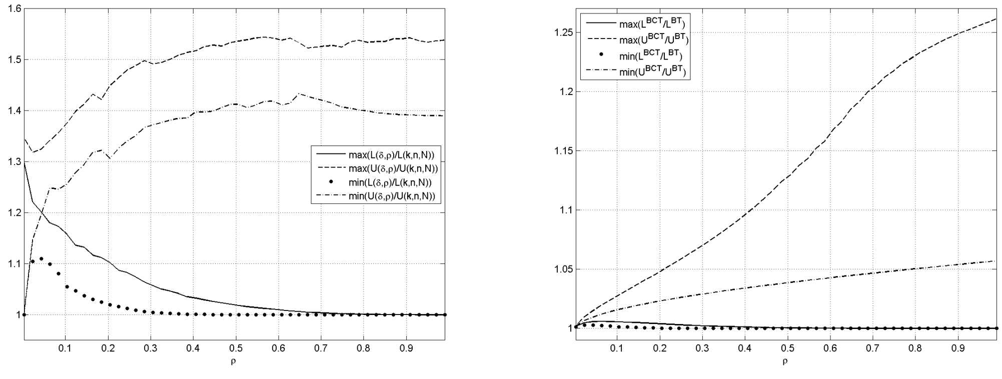

Figure 2.5: *Left panel:* The maximum and minimum, over $\delta$, sharpness ratios, $\frac{\mathcal{U}^{BT}(\delta,\rho)}{U(k,n,N;A)}$ and $\frac{\mathcal{L}^{BT}(\delta,\rho)}{L(k,n,N;A)}$ as a function of $\rho$; with the maximum and minimum taken over all $\delta \in [0.05, 0.9524]$, the same $\delta$ values used in Figure 2.4. *Right panel:* The maximum and minimum, over $\delta$, improvement ratios over the previous best known bounds, $\frac{\mathcal{U}^{BCT}(\delta,\rho)}{\mathcal{U}^{BT}(\delta,\rho)}$ and $\frac{\mathcal{L}^{BCT}(\delta,\rho)}{\mathcal{L}^{BT}(\delta,\rho)}$ as a function of $\rho$, with the maximum and minimum also taken over $\delta \in [0.05, 0.9524]$.

over $\delta \in [0.05, 0.9524]$.

Removing the optimization of $\gamma \in [\rho, \delta^{-1}]$ in Definition 2.3.1 and fixing $\gamma = \rho$ recovers the bounds on $L(k, n, N; A)$ and the first of two bounds on $U(k, n, N; A)$ presented in [19]. The first bound on $U(k, n, N; A)$ in [19] suffers from excessive overestimation when $\delta\rho \approx 1/2$ because of the combinatorial term. In fact, this overestimation is so severe that for some $(\delta, \rho)$ with $\delta\rho \approx 1/2$, smaller bounds are obtained at $(\delta, 1)$. This overestimation is somewhat ameliorated by noting the monotonicity of $U(k, n, N; A)$ in $k$, obtaining the improved bound, see (2.6).

### 2.3.1 Discussion on the Construction of Improved $\mathrm{RIC}_2$ Bounds

The bounds in Theorem 2.3.2 improve upon the earlier results of [19] by grouping matrices $A_K$ and $A_{K'}$ that share a significant number of columns from $A$. This is manifest in Definition 2.3.1 through the introduction of the free parameter $\gamma$ associated with the number of groups considered. In this section we first discuss the way in which we construct these groups and the sense in which the bounds in Theorem 2.3.2 are optimal for this construction. Equipped with a suitable construction of groups, we discuss the way in which this grouping is employed to improve the $\mathrm{RIC}_2$ bounds from [19].

**Construction of Groups**

We construct our groups of $A_K$ by selecting a subset $M_i$ from $\{1, 2, \ldots, N\}$ of cardinality $|M_i| = m \geq k$ and setting $\mathcal{G}_i := \{K\}_{K\subset M_i, |K|=k}$, the set of all sets $K \subset M_i$ of cardinality $k$. The group $\mathcal{G}_i$ has $\binom{m}{k}$ members, with any two members sharing at least $2k-m$ elements. Hence, the quantity $\gamma = m/n$ in Definition 2.3.1 is associated with the cardinality of the groups $\mathcal{G}_i$. In order to calculate bounds on the $\mathrm{RIC}_2$ of a matrix, we need a collection of groups whose union includes all $\binom{N}{k}$ sets of cardinality $k$ from $\Omega := \{1, 2, \ldots, N\}$; that is, we need $\{\mathcal{G}_i\}_{i=1}^{u}$ such that $G := \bigcup_{i=1}^{u} \mathcal{G}_i$ with $|G| \geq \binom{N}{k}$. From simple counting, the minimum number of groups $\mathcal{G}_i$ needed for this covering is at least $r := \binom{N}{k}\binom{m}{k}^{-1}$. Although the construction of a minimal covering is an open question [88], even a simple random construction of the $\mathcal{G}_i$'s requires typically only a polynomial multiple of $r$ groups, hence achieving the optimal large deviation rate. This claim is formalised in Lemma 2.3.3 and Corollary 2.3.4.

**Lemma 2.3.3** ([88]). *Set $r = \binom{N}{k}\binom{m}{k}^{-1}$ and draw $u := rN$ sets $M_i$ each of cardinality $m$, drawn uniformly at random from the $\binom{N}{m}$ possible sets of cardinality $m$. With $G$ defined as above,*

$$\textit{Prob}\left(|G| < \binom{N}{k}\right) < C(k/N) \cdot N^{-1/2} \cdot e^{-N(1-\ln 2)}, \tag{2.10}$$

*where $C(p) \leq \frac{5}{4}(2\pi p(1-p))^{-\frac{1}{2}}$.*

*Proof.* Select one set $K \subset \Omega$ of cardinality $|K| = k$ prior to the draw of the sets $M_i$. The probability that it is not contained in one set $M_i$ is $1/r$, and with each $M_i$ drawn independently, the probability that it is not contained in any of the $u$ $M_i$ sets is $(1 - r^{-1})^u \leq e^{-u/r}$. Applying a union bound over all $\binom{N}{k}$ sets $K$ yields

$$\text{Prob}\left(|G| < \binom{N}{k}\right) < \binom{N}{k} e^{-u/r}.$$

Noting from Stirling's Inequality [1] that

$$\frac{16}{25}(2\pi p(1-p)N)^{-\frac{1}{2}} e^{N\mathrm{H}(p)} \leq \binom{N}{pN} \leq \frac{5}{4}(2\pi p(1-p)N)^{-\frac{1}{2}} e^{N\mathrm{H}(p)}, \tag{2.11}$$

with $\mathrm{H}(p) \leq \ln 2$ for $p \in [0, 1]$, and substituting the selected value of $u$ completes the proof. Note that an exponentially small probability can be obtained with $u$ just larger than $rNH(\delta\rho)$, but the smaller polynomial factor is negligible for our purposes. □

**Corollary 2.3.4.** *In the proportional-growth asymptotics, the probability that all the $\binom{N}{k}$ $K$ subsets of $\{1, 2, \ldots, N\}$ are covered by $G$ converges to one exponentially in $n$.*

*Proof.* Given in Lemma 2.3.3, as $n \to \infty$ the right hand side of (2.10) goes to zero exponentially in $n$ and this is equivalent to the statement of the corollary. □

### Decreasing the Combinatorial Term

We illustrate the way the groups $\mathcal{G}_i$ are used to improve the bound on the upper RIC$_2$ $U(k, n, N; A)$; the bounds for $L(k, n, N; A)$ following by a suitable replacement of maximizations/minimizations and sign changes. All previous bounds on the RIC$_2$ for the Gaussian ensemble have overcome the combinatorial maximization/minimization by use of a union bound over all $\binom{N}{k}$ sets $K \subset \Omega$ and then using a tail bound on the PDF of the extreme eigenvalues of

$A_K^* A_K$; for some $\lambda_{\max}^* > 0$,

$$\text{Prob}\left(\max_{K\subset\Omega,|K|=k} \lambda^{\max}\left(A_K^* A_K\right) > \lambda_{\max}^*\right) \le \binom{N}{k} \text{Prob}\left(\lambda^{\max}\left(A_K^* A_K\right) > \lambda_{\max}^*\right).$$

That the random variables $\lambda^{\max}\left(A_K^* A_K\right)$ are treated as independent is the principal deficiency of this bound. To exploit dependencies of this variable for $K$ and $K^{'}$ with significant overlap we exploit the groupings $\mathcal{G}_i$, which, at least for $m$ moderately larger than $k$, contain sets with significant overlap. For the moment we assume the groups $\{\mathcal{G}_i\}_{i=1}^u$ cover all $K \subset \Omega$, and replace the above maximization over $K$ with a double maximization

$$\text{Prob}\left(\max_{K\subset\Omega,|K|=k} \lambda^{\max}\left(A_K^* A_K\right) > \lambda_{\max}^*\right) = \text{Prob}\left(\max_{i=1,\dots,u}\max_{K\subset\mathcal{G}_i,|K|=k} \lambda^{\max}\left(A_K^* A_K\right) > \lambda_{\max}^*\right).$$

The outer maximization can be bounded over all $u$ sets $\mathcal{G}_i$, again, using a simple union bound; however, with a smaller combinatorial term.

The expected dependencies between $\lambda^{\max}\left(A_K^* A_K\right)$ for $K \subset \mathcal{G}_i$ can, at times, be better controlled by replacing the maximization over $K \subset \mathcal{G}_i$ by $\lambda^{\max}\left(A_{M_i}^* A_{M_i}\right)$ where $M_i$ is the subset of cardinality $m$ containing all $K \subset \mathcal{G}_i$:

$$\text{Prob}\left(\max_{i=1,\dots,u}\max_{K\subset\mathcal{G}_i,|K|=k} \lambda^{\max}\left(A_K^* A_K\right) > \lambda_{\max}^*\right) \le u\cdot\text{Prob}\left(\lambda^{\max}\left(A_{M_i}^* A_{M_i}\right) > \lambda_{\max}^*\right). \quad (2.12)$$

Selecting $m = k$ recovers the usual union bound with $u$ equal to $\binom{N}{k}$. Larger values of $m$ decrease the combinatorial term at the cost of increasing $\lambda^{\max}\left(A_{M_i}^* A_{M_i}\right)$. The efficacy of this approach depends on the interplay between these two competing factors. In the proportional-growth asymptotic, this interplay is observed through the optimization over $\frac{m}{n} = \gamma \in [\rho, \delta^{-1}]$. Definition 2.3.1 uses the tail bounds on the extreme eigenvalues of Wishart Matrices derived by Edelman [62] to bound $\text{Prob}\left(\lambda^{\max}\left(A_{M_i}^* A_{M_i}\right) > \lambda_{\max}^*\right)$. The previously best known bound on the RIC$_2$ for the Gaussian ensemble is recovered by selecting $\gamma = \rho$ in Definition 2.3.1, [19]. This is illustrated in Figure 2.6. The innovation of the bounds in Theorem 2.3.2 follows from there always being a unique $\gamma > \rho$ such that $\lambda^{\max}(\delta, \rho; \gamma)$ is less than $\lambda^{\max}(\delta, \rho; \rho)$. Lemma 2.3.5 confirms this.

**Lemma 2.3.5.** *Suppose $\lambda^{\min}(\delta, \rho; \gamma)$ and $\lambda^{\max}(\delta, \rho; \gamma)$ are solutions to (2.7) and (2.8) respectively. For any fixed $(\delta, \rho)$ there exist a unique $\gamma_{\min} \in [\rho, \delta^{-1}]$ that minimizes $\lambda^{\max}(\delta, \rho; \gamma)$ and a unique $\gamma_{\max} \in [\rho, \delta^{-1}]$ that maximizes $\lambda^{\min}(\delta, \rho; \gamma)$. Furthermore, $\gamma_{\min}$ and $\gamma_{\max}$ are strictly larger than $\rho$.*

Corollary 2.3.6 follows from this lemma. The optimal choices of $\gamma$ depicted by $\gamma - \rho$ for $\mathcal{U}^{BT}(\rho, \delta)$ and $\mathcal{L}^{BT}(\rho, \delta)$ in $(\rho, \delta) \in (0, 1)^2$ are displayed in Figure 2.7. The proof of Lemma 2.3.5 is presented in Section 2.6.1.

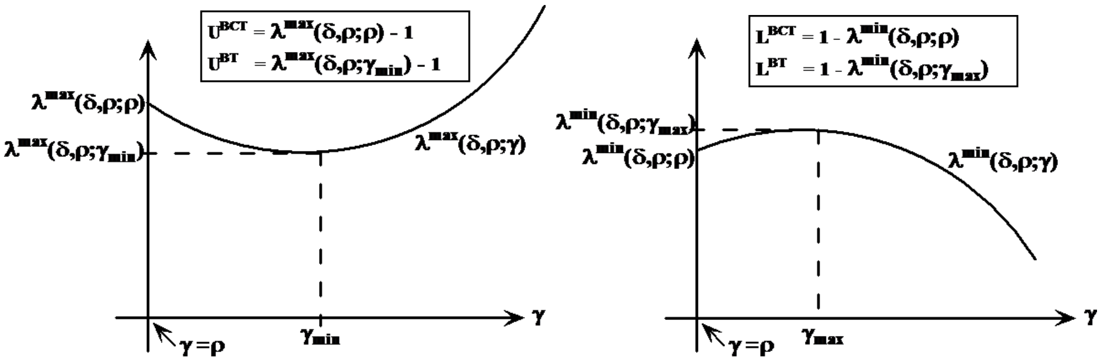

Figure 2.6: *Left panel:* The relationship between the new bound $\mathcal{U}^{BT}(\delta,\rho)$, Theorem 2.3.2, and the previous smallest bound $\mathcal{U}^{BCT}(\delta,\rho)$, Theorem 2.2.4, where in the two bounds $\lambda^{\max}(\delta,\rho;\gamma)$ is evaluated at $\gamma=\gamma_{\min}$ and $\gamma=\rho$ respectively. *Right panel:* The relationship between the new bound $\mathcal{L}^{BT}(\delta,\rho)$, Theorem 2.3.2, and the previous smallest bound $\mathcal{L}^{BCT}(\delta,\rho)$, Theorem 2.2.4, where in the two bounds $\lambda^{\min}(\delta,\rho;\gamma)$ is evaluated at $\gamma=\gamma_{\max}$ and $\gamma=\rho$ respectively.

**Corollary 2.3.6.** *Let $\mathcal{L}^{BT}(\delta,\rho)$ and $\mathcal{U}^{BT}(\delta,\rho)$ be defined as in Definition 2.3.1 and the* RIC$_2$ *bounds $\mathcal{L}^{BCT}(\delta,\rho)$ and $\mathcal{U}^{BCT}(\delta,\rho)$ be defined as in Definition 2.2.3. For any fixed $(\delta,\rho)\in(0,1)^2$,*

$$\mathcal{L}^{BT}(\delta,\rho)<\mathcal{L}^{BCT}(\delta,\rho) \quad \textit{and} \quad \mathcal{U}^{BT}(\delta,\rho)<\mathcal{U}^{BCT}(\delta,\rho). \tag{2.13}$$

*Proof.* Lemma 2.3.5 implies that $\lambda^{\max}_{BT}(\delta,\rho)<\lambda^{\max}_{BCT}(\delta,\rho)$ resulting in the statement of the corollary for $\mathcal{U}^{BT}(\delta,\rho)$ in (2.13). Similarly for $\mathcal{L}^{BT}(\delta,\rho)$ in (2.13). □

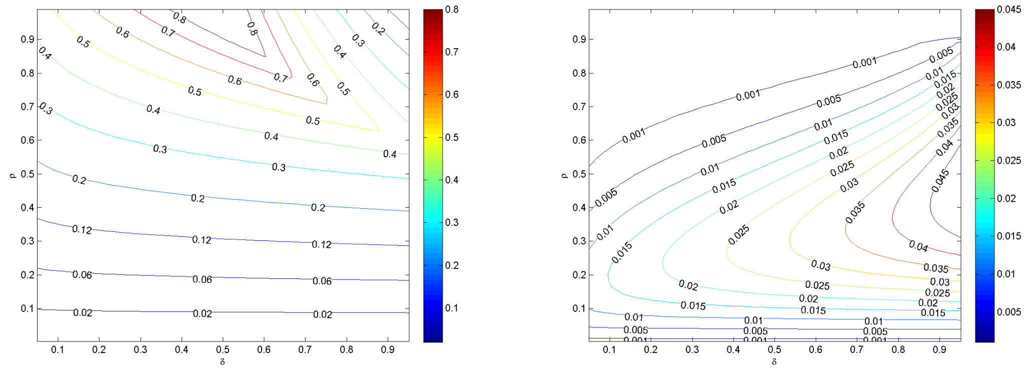

Figure 2.7: Optimal choice of $\gamma$ depicted by the error $\gamma-\rho$ for, *left panel:* $\mathcal{U}^{BT}(\delta,\rho)$ and *right panel:* $\mathcal{L}^{BT}(\delta,\rho)$.

## 2.4 Finite $N$ Interpretations

The method of proof used to obtain the proportional-growth asymptotic bounds in Theorem 2.3.2 also provides, albeit less elegantly, bounds valid for finite values of $(k,n,N)$ and specified probabilities of the bound being satisfied. Given a problem instance $(k,n,N)$ and

$\epsilon$, bounds on the tail probabilities of the RIC$_2$, Prob$\big(U(k,n,N;A) > \mathcal{U}^{BT}(\delta_n,\rho_n)+\epsilon\big)$ and Prob$\big(L(k,n,N;A) > \mathcal{L}^{BT}(\delta_n,\rho_n)+\epsilon\big)$, for discrete values of $\delta$ and $\rho$ are given in Propositions 2.4.1 and 2.4.2 respectively.

**Proposition 2.4.1.** *Let $A$ be a matrix of size $n \times N$ whose entries are drawn i.i.d. from $\mathcal{N}(0,1/n)$. Define $\mathcal{U}^{BT}(\delta_n,\rho_n)$ as in Definition 2.3.1 for discrete values of $\delta$ and $\rho$. Then for any $\epsilon > 0$,*

$$\begin{aligned}\textit{Prob}\big(U(k,n,N;A) > \mathcal{U}^{BT}(\delta_n,\rho_n)+\epsilon\big) &\le p'_{\max}\left(n,\lambda^{\max}(\delta_n,\rho_n)\right)\times \\ \exp\left(n\epsilon\cdot\frac{d}{d\lambda}\psi_U\left(\lambda^{\max}(\delta_n,\rho_n)\right)\right) &+ \frac{5}{4}(2\pi k(1-k/N))^{-1/2}\exp(-N(1-\ln 2)),\end{aligned}$$

*where*

$$p'_{\max}(n,\lambda) := \left(\frac{8}{\pi}\right)^{1/2}\frac{2n^{-7/2}}{\sqrt{\gamma\lambda}}\left(\frac{5}{4}\right)^{3}\left(\frac{nN(\gamma-\rho)}{\gamma\delta(1-\rho\delta)}\right)^{1/2}, \tag{2.14}$$

*and*

$$\psi_U(\lambda,\gamma) := \delta^{-1}\left[H(\rho\delta) - \delta\gamma H\left(\frac{\rho}{\gamma}\right) + \delta\psi_{\max}(\lambda,\gamma)\right] \tag{2.15}$$

*for $\psi_{\max}(\lambda,\gamma)$ defined in* (2.3).

**Proposition 2.4.2.** *Let $A$ be a matrix of size $n \times N$ whose entries are drawn i.i.d. from $\mathcal{N}(0,1/n)$. Define $\mathcal{L}^{BT}(\delta_n,\rho_n)$ as in Definition 2.3.1 for discrete values of $\delta$ and $\rho$. Then for any $\epsilon > 0$,*

$$\begin{aligned}\textit{Prob}\big(L(k,n,N;A) > \mathcal{L}^{BT}(\delta_n,\rho_n)+\epsilon\big) &\le p'_{\min}\left(n,\lambda^{\min}(\delta_n,\rho_n)\right)\times \\ \exp\left(n\epsilon\cdot\frac{d}{d\lambda}\psi_L\left(\lambda^{\min}(\delta_n,\rho_n)\right)\right) &+ \frac{5}{4}(2\pi k(1-k/N))^{-1/2}\exp(-N(1-\ln 2)),\end{aligned} \tag{2.16}$$

*where*

$$p'_{\min}(n,\lambda) := \left(\frac{5}{4}\right)^{3}\frac{e\sqrt{\lambda}}{\pi\sqrt{2}}\left(\frac{nN(\gamma-\rho)}{\gamma\delta(1-\rho\delta)}\right)^{1/2}, \tag{2.17}$$

*and*

$$\psi_L(\lambda,\gamma) := \delta^{-1}\left[H(\rho\delta) - \delta\gamma H\left(\frac{\rho}{\gamma}\right) + \delta\psi_{\min}(\lambda,\gamma)\right] \tag{2.18}$$

*for $\psi_{\min}(\lambda,\gamma)$ defined in* (2.2).

The proofs of Propositions 2.4.1 and 2.4.2 are presented in Section 2.6.2 and also serve as the proof of Theorem 2.3.2, that follows by taking the appropriate limits. From Propositions 2.4.1 and 2.4.2 we calculated bounds for a few example values of $(k,n,N)$ and $\epsilon$. Table 2.1 shows bounds on Prob$\big(U(k,n,N;A) > \mathcal{U}^{BT}(\delta_n,\rho_n)+\epsilon\big)$ for a few values of $(k,n,N)$ with two different choices of $\epsilon$. It is remarkable that these probabilities are already close to zero for these small values of $(k,n,N)$ and even for $\epsilon \ll 1$. Table 2.2 shows bounds on Prob$\big(L(k,n,N;A) > \mathcal{L}^{BT}(\delta_n,\rho_n)+\epsilon\big)$ for the same values of $(k,n,N)$ as in Table 2.1, but with even smaller values for $\epsilon$. Again, it is remarkable that these probabilities are extremely small, even for relatively small values of $(k, n, N)$ and $\epsilon$.

| $k$ | $n$ | $N$ | $\epsilon$ | *prob* |
|---|---|---|---|---|
| 100 | 200 | 2000 | $10^{-3}$ | $2.9 \times 10^{-2}$ |
| 200 | 400 | 4000 | $10^{-3}$ | $9.5 \times 10^{-3}$ |
| 400 | 800 | 8000 | $10^{-3}$ | $2.9 \times 10^{-3}$ |
| 100 | 200 | 2000 | $10^{-10}$ | $3.2 \times 10^{-2}$ |
| 200 | 400 | 4000 | $10^{-10}$ | $1.1 \times 10^{-2}$ |
| 400 | 800 | 8000 | $10^{-10}$ | $4.0 \times 10^{-3}$ |

Table 2.1: The probability of the upper RIC$_2$ bound failing to be true for finite problem sizes $(k, n, N)$, where *prob* is an upper bound on Prob$\left(U(k,n,N;A) > \mathcal{U}^{BT}(\delta_n, \rho_n) + \epsilon\right)$ for the specified $(k, n, N)$ and $\epsilon$.

| $k$ | $n$ | $N$ | $\epsilon$ | *prob* |
|---|---|---|---|---|
| 100 | 200 | 2000 | $10^{-5}$ | $2.8 \times 10^{-18}$ |
| 200 | 400 | 4000 | $10^{-5}$ | $9.1 \times 10^{-32}$ |
| 400 | 800 | 8000 | $10^{-5}$ | $2.8 \times 10^{-58}$ |

Table 2.2: The probability of the lower RIC$_2$ bound failing to be true for finite problem sizes $(k, n, N)$, where *prob* is an upper bound on Prob$\left(L(k,n,N;A) > \mathcal{L}^{BT}(\delta_n, \rho_n) + \epsilon\right)$ for the specified $(k, n, N)$ and $\epsilon$.

## 2.5 Implications for Compressed Sensing

The RIC$_2$ were introduced by Candès and Tao [39] as a technique to prove that in certain conditions the sparsest solution of the underdetermined system of equations (1.1) can be found using linear programming. The RIC$_2$ is now a widely used technique in the study of sparse approximation algorithms, allowing the analysis of sparse approximation algorithms without specifying the measurement matrix $A$. For instance, Candès and Tao [39] proved that if $R(2k,n,N;A) + R(3k,n,N;A) < 1$, where $R(\cdot,n,N;A) = \max\left(L(\cdot,n,N;A), U(\cdot,n,N;A)\right)$ as in (1.6), and if (1.1) or equivalently (1.12) has a unique $k$-sparse solution as its sparsest solution, then the solution to (1.17) will be this $k$-sparse solution. The sufficient condition for robust and stable recovery of $k$-sparse vectors by $\ell_1$-minimization was improved several times including Candès, Romberg and Tao [32] improving it to $R(3k,n,N;A) + R(4k,n,N;A) < 2$ and Candès [37] came up with $R(2k,n,N;A) < \sqrt{2}-1$. The best improvement on this condition is due to Mo and Li in [105] which is $R(2k,n,N;A) < 0.4931$, while other improvements can be found in [68, 67].

For compressed sensing greedy algorithms such conditions include $R(3k,n,N;A) < 1/\sqrt{8}$ for Iterative Hard Thresholding (IHT) [25] and $R(4k,n,N;A) < 0.1$ for Compressive Sampling Matching Pursuit (CoSaMP) [109]. A host of other RIC$_2$ based conditions have been derived for $\ell_1$-minimization and other sparsifying algorithms. One gets the impression that the smaller the sparsity the better the condition. In fact Blanchard and Thompson showed in [22] the sparsity $2k$ is not necessarily the best option for Gaussian random matrices. Moreover, the values of $(k, n, N)$ when these conditions on the $\text{RIC}_2$ are satisfied can only be determined once the measurement matrix $A$ has been specified [23].

### 2.5.1 Phase Transitions of Compressed Sensing Algorithms

In [20], using $\text{RIC}_2$ bounds from [19], lower bounds on the phase transitions for exact recovery of $k$-sparse signals for three greedy algorithms and $l_1$-minimization were presented. These curves are functions $\rho_S^{sp}(\delta)$ for Subspace Pursuit (SP) [50], $\rho_S^{csp}(\delta)$ for Compressive Sampling Matching Pursuit (CoSaMP) [109], $\rho_S^{iht}(\delta)$ for Iterative Hard Thresholding (IHT) [25], and $\rho_S^{l_1}(\delta)$ for $l_1$-minimisation [68]. From Theorem 2.5.1 and Corollary 2.5.2 Blanchard et al in [20] derived bounds for the afore mentioned phase transition functions using the BCT $\text{RIC}_2$ bounds.

**Theorem 2.5.1** ([20])**.** *Given a matrix $A$ with entries drawn i.i.d. from $\mathcal{N}(0, 1/n)$, for any $x \in \chi^N(k)$, let $y = Ax + e$ for some (unknown) noise vector $e$. For any $\epsilon \in (0, 1)$, as $(k, n, N) \to \infty$ with $n/N \to \delta \in (0, 1)$ and $k/n \to \rho \in (0, 1)$, there exists $\mu^{alg}(\delta, \rho)$ and $\rho_S^{alg}(\delta)$, the unique solution to $\mu^{alg}(\delta, \rho) = 1$. If $\rho < (1 - \epsilon)\rho_S^{alg}(\delta)$, there is exponentially high probability on the draw of $A$ that the output of the algorithm at the $l^{th}$ iteration, $\hat{x}$, approximates $x$ within the bound*

$$\|x - \hat{x}\|_2 \leq \kappa^{alg}\left(\delta, (1 - \epsilon)\rho\right)\left[\mu^{alg}\left(\delta, (1 - \epsilon)\rho\right)\right]^l \|x\|_2 + \frac{\xi^{alg}\left(\delta, (1 - \epsilon)\rho\right)}{1 - \mu^{alg}\left(\delta, (1 - \epsilon)\rho\right)}\|e\|_2,$$

*for some $\kappa^{alg}(\delta, \rho)$ and $\xi^{alg}(\delta, \rho)$.*

**Corollary 2.5.2** ([20])**.** *Given a matrix $A$ with entries drawn i.i.d. from $\mathcal{N}(0, 1/n)$, for any $x \in \chi^N(k)$, let $y = Ax$. For any $\epsilon \in (0, 1)$, with $n/N \to \delta \in (0, 1)$ and $k/n \to \rho < (1 - \epsilon)\rho_S^{alg}(\delta)$ as $(k, n, N) \to \infty$, there is an exponentially high probability on the draw of $A$ that the algorithm exactly recovers $x$ from $y$ and $A$ in a finite number of iterations not to exceed*

$$l_{\max}^{alg}(x) := \left\lceil \frac{\log\left(\nu_{\min}(x)\right)}{\log\left(\mu^{alg}(\delta, \rho)\right)} \right\rceil + 1 \quad \textit{where} \quad \nu_{\min}(x) := \frac{\min_{i \in T} |x_i|}{\|x\|_2}$$

*with $T := \{i : x_i \neq 0\}$ and $\lceil m \rceil$, the smallest integer greater than or equal to $m$.*

Corollary 2.5.2 provides *strong* phase transition curves, $\rho_S^{alg}(\delta)$, below which the algorithm can be guaranteed to converge provided there is such an $x \in \chi^N(k)$ that satisfies (1.1). Blanchard et al in [20] derived expressions for the bound on the convergence factor and the stability factors , $\mu^{alg}(\delta, \rho)$ and $\frac{\xi^{alg}(\delta, \rho)}{1 - \mu^{alg}(\delta, \rho)}$, respectively. Note that $\rho_S^{alg}(\delta)$ corresponds to the bound $\mu^{alg}(\delta, \rho) = 1$. Below we state part of theorems involving $\mu^{alg}(\delta, \rho)$ for a few algorithms, where $\mathcal{L}(\delta, \rho)$ and $\mathcal{U}(\delta, \rho)$ are bounds of $L(k, n, N; A)$ and $U(k, n, N; A)$ respectively.

### Compressive Sampling Matching Pursuit (CoSaMP)

CoSaMP is one of the greedy algorithms that iteratively identifies the correct support set. Specifically it choose the support set with the largest (in magnitude) $k$ entries when the pseudoinverse, $A^\dagger$ is applied to $y$. The transpose of $A$, $A^T$ is applied to the residual of the previous iteration and a hard threshold of the largest $2k$ is used to form $A^\dagger$. Algorithm 1 in Table 2.3 is a pseudocode of CoSaMP. Theorem 2.5.3 gives an expression for $\mu^{csp}(\delta,\rho)$ and $\kappa^{csp}(\delta,\rho)$ for CoSaMP.

```
Input: $A$, $y$, $k$
Output: $k$-sparse approximation $\hat{x}$ of the target signal $x$
Initialization:
  1. Set $\Lambda^0 = 0$
  2. Set $y^0 = 0$
Iteration: During iteration $l$, do
  1. $\tilde{\Lambda}^l = \Lambda^{l-1} \cup \{k$ indices of the largest magnitude entries of $A^T y^{l-1}\}$
  2. $\tilde{x} = A^\dagger_{\tilde{\Lambda}^l} y$
  3. $\Lambda^l = \{k$ indices of the largest magnitude entries of $\tilde{x}\}$
  4. $y^l = y - A_{\Lambda^l}\tilde{x}_{\Lambda^l}$
  5. if $\|y^l\|_2 = 0$ then
  6.     return $\hat{x}$ defined by $\hat{x}_{\{1,\dots,N\}\setminus\Lambda^l} = 0$ and $\tilde{x}_{\Lambda^l} = \hat{x}_{\Lambda^l}$
  7. else
  8.     Perform iteration $l+1$
  9. end if
```

Table 2.3: **Algorithm 1** – Compressive Sampling Matching Pursuit (CoSaMP) [109].

**Theorem 2.5.3** (Theorem 10 [20])**.** *CoSaMP, Algorithm 1, satisfies Theorem 2.5.1 and Corollary 2.5.2 with $\kappa^{csp}(\delta,\rho) := 1$ and $\mu^{csp}(\delta,\rho)$ defined as*

$$\mu^{csp}(\delta,\rho) := \frac{1}{2}\left(2 + \frac{\mathcal{L}(\delta,4\rho) + \mathcal{U}(\delta,4\rho)}{1-\mathcal{L}(\delta,3\rho)}\right)\left(\frac{\mathcal{L}(\delta,2\rho) + \mathcal{U}(\delta,2\rho) + \mathcal{L}(\delta,4\rho) + \mathcal{U}(\delta,4\rho)}{1-\mathcal{L}(\delta,2\rho)}\right).$$

### Subspace Pursuit (SP)

Similar to CoSaMP, SP chooses the support set with the largest (in magnitude) $k$ entries when the pseudoinverse, $A^\dagger$ is applied $y$. $A^T$ is applied to the residual of the previous iteration and a hard threshold of the largest $k$ is used to form $A^\dagger$. However, unlike CoSaMP the identification of the columns of the submatrices for $A^\dagger$ involves another pseudoinverse which is a disadvantage of SP. Algorithm 2 of Table 2.4 is a pseudocode of SP. Theorem 2.5.4 gives an expression for $\mu^{sp}(\delta,\rho)$ and $\kappa^{sp}(\delta,\rho)$ for SP.

**Theorem 2.5.4** (Theorem 11 [20])**.** *Theorem 2.5.1 and Corollary 2.5.2 are satisfied by SP, Algorithm 2, with $\kappa^{sp}(\delta,\rho) := 1 + \frac{\mathcal{U}(\delta,2\rho)}{1-\mathcal{L}(\delta,\rho)}$ and $\mu^{sp}(\delta,\rho)$ defined as*

$$\mu^{sp}(\delta,\rho) := \frac{2\mathcal{U}(\delta,3\rho)}{1-\mathcal{L}(\delta,\rho)} \cdot \left(1 + 2\frac{\mathcal{U}(\delta,3\rho)}{1-\mathcal{L}(\delta,2\rho)}\right) \cdot \left(1 + \frac{\mathcal{U}(\delta,2\rho)}{1-\mathcal{L}(\delta,\rho)}\right).$$

```
**Input:** $A,\ y,\ k$
**Output:** $k$-sparse approximation $\hat{x}$ of the target signal $x$
**Initialization:**
  1. Set $\Lambda^0 = \{k$ indices of the largest magnitude entries of $A^T y$
  2. Set $y_r^0 = y - A_{\Lambda^0} A_{\Lambda^0}^{\dagger} y$
**Iteration:** During iteration $l$, **do**
  1. $\tilde{\Lambda}^l = \Lambda^{l-1} \cup \{2k$ indices of the largest magnitude entries of $A^T y_r^{l-1}\}$
  2. $\tilde{x} = A_{\tilde{\Lambda}^l}^{\dagger} y$
  3. $\Lambda^l = \{k$ indices of the largest magnitude entries of $\tilde{x}\}$
  4. $y_r^l = y - A_{\Lambda^l} A_{\Lambda^l}^{\dagger} y$
  5. **if** $\|y_r^l\|_2 = 0$ **then**
  6.     **return** $\hat{x}$ defined by $\hat{x}_{\{1,\dots,N\}\setminus\Lambda^l} = 0$ and $\hat{x}_{\Lambda^l} = A_{\Lambda^l}^{\dagger} y$
  7. **else**
  8.     Perform iteration $l + 1$
  9. **end if**
```

Table 2.4: **Algorithm 2** – Subspace Pursuit (SP) [50]

### Iterative Hard Thresholding (IHT)

IHT is also a greedy algorithm but unlike the above two it recovers the support set by taking the largest (in magnitude) entries of the approximation of the target signal instead of the residual. Algorithm 3 of Table 2.5 is a pseudocode of IHT. Theorem 2.5.5 gives an expression for $\mu^{iht}(\delta,\rho)$, $\kappa^{iht}(\delta,\rho)$ and $\omega$ for IHT.

```
**Input:** $A,\ y,\ \omega \in (0,1),\ k$
**Output:** $k$-sparse approximation $\hat{x}$ of the target signal $x$
**Initialization:**
  1. Set $x^0 = 0$
  2. Set $\Lambda^0 = \emptyset$
  3. Set $y^0 = y$
**Iteration:** During iteration $l$, **do**
  2. $x^l = x_{\Lambda^{l-1}}^{l-1} + \omega A^T y^{l-1}$
  3. $\Lambda^l = \{k$ indices of the largest magnitude entries of $x^l\}$
  4. $y^l = y - A_{\Lambda^l} x_{\Lambda^l}^l$
  5. **if** $\|y^l\|_2 = 0$ **then**
  6.     **return** $\hat{x}$ defined by $\hat{x}_{\{1,\dots,N\}\setminus\Lambda^l} = 0$ and $\hat{x}_{\Lambda^l} = x_{\Lambda^l}^l$
  7. **else**
  8.     Perform iteration $l + 1$
  9. **end if**
```

Table 2.5: **Algorithm 3** – Iterative Hard Thresholding (IHT) [25]

**Theorem 2.5.5** (Theorem 12 [20]). *Theorem 2.5.1 and Corollary 2.5.2 are satisfied by IHT, Algorithm 3, with* $\omega := \frac{2}{2+\mathcal{U}(\delta,3\rho)-\mathcal{L}(\delta,3\rho)}$, $\kappa^{iht}(\delta,\rho) := 1$ *and* $\mu^{iht}(\delta,\rho)$ *defined as*

$$\mu^{iht}(\delta,\rho) := 2\sqrt{2}\left(\frac{\mathcal{L}(\delta,3\rho)+\mathcal{U}(\delta,3\rho)}{2+\mathcal{U}(\delta,3\rho)-\mathcal{L}(\delta,3\rho)}\right).$$

### $\ell_1$-minimization

This approach is a relaxation of the $\ell_0$-minimisation problem and it has lots of algorithms that are generic linear programming algorithms and others that are specifically designed for compressed sensing. Recovery guarantees for the so called $\ell_1/\ell_0$ *equivalence* has been developed from RIC$_2$ [68], convex polytopes [56] and geometric functional analysis [121]. A detailed work on this was done in [19] and the equivalence of Theorem 2.5.1 and Corollary 2.5.2 were derived respectively as the following.

**Theorem 2.5.6** (Theorem 13 [20])**.** *Given a matrix $A$ with entries drawn i.i.d. from $\mathcal{N}(0,1/n)$, for any $x \in \chi^N(k)$, let $y = Ax + e$ for some (unknown) noise vector $e$. Define*

$$\mu^{\ell_1}(\delta,\rho) := \frac{1+\sqrt{2}}{4}\left(\frac{1+\mathcal{L}(\delta,2\rho)}{1-\mathcal{L}(\delta,2\rho)} -\right) \quad \text{and} \quad \xi^{\ell_1}(\delta,\rho) := \frac{3\left(1+\sqrt{2}\right)}{1-\mathcal{L}(\delta,2\rho)}.$$

*Let $\rho_S^{\ell_1}(\delta)$ be the unique solution to $\mu^{\ell_1}(\delta,\rho) = 1$. For any $\epsilon > 0$, as $(k,n,N) \to \infty$ with $n/N \to \delta \in (0,1)$ and $k/n \to \rho < (1-\epsilon)\rho_S^{\ell_1}(\delta)$, there is an exponentially high probability on the draw of $A$ that*

$$\hat{x} := \arg\min_z \|z\|_1 \quad \text{subject to} \quad \|Az - y\|_2 \le \|e\|_2$$

*approximates $x$ within the bound*

$$\|x - \hat{x}\|_2 \le \frac{\xi\left(\delta,(1-\epsilon)\rho\right)}{1-\mu\left(\delta,(1-\epsilon)\rho\right)}\|e\|_2.$$

**Corollary 2.5.7** (Corollary 14 [20])**.** *For a matrix $A$ with entries drawn i.i.d. from $\mathcal{N}(0,1/n)$, for any $x \in \chi^N(k)$, let $y = Ax$. Given any $\epsilon \in (0,1)$, with $k/n \to \rho < (1-\epsilon)\rho_S^{\ell_1}(\delta)$ and $n/N \to \delta \in (0,1)$ as $(k,n,N) \to \infty$, there is an exponentially high probability on the draw of $A$ that*

$$\hat{x} := \arg\min_z \|z\|_1 \quad \text{subject to} \quad Az = y$$

*exactly recovers $x$ from $y$ and $A$.*

Figure 2.8 shows a plot of these strong phase transition curves and their inverse based on our new bounds, i.e. $\mathcal{L}(\cdot)$ and $\mathcal{U}(\cdot)$ in Theorems 2.5.3 – 2.5.6 are our bounds. Theorems 2.5.3 – 2.5.6 basically present lower bounds on the algorithmic exact sparse recovery phase transitions. The curves on the left panel of Figure 2.8 are defined by functions $\rho_S^{\ell_1}(\delta)$ ($\ell_1$-minimization the blue curve), $\rho_S^{iht}(\delta)$ (Iterative Hard Thresholding the red curve), $\rho_S^{sp}(\delta)$ (Subspace Pursuit the magenta curve), and $\rho_S^{csp}(\delta)$ (CoSaMP the black curve). From Figure 2.8 we are able to directly compare the provable recovery results of the three greedy algorithms as well as $\ell_1$-minimization. For a given problem instance $(k,n,N)$ with the entries of $A$ drawn i.i.d. from $\mathcal{N}(0,1/n)$, if $k/n = \rho$ falls in the region below the curve $\rho_S^{alg}(\delta)$ for a specific algorithm, then with probability approaching 1 exponentially in $n$, the algorithm will exactly recover the $k$-

sparse vector $x \in \chi^N(k)$ irrespective of which $x \in \chi^N(k)$ was measured by A.

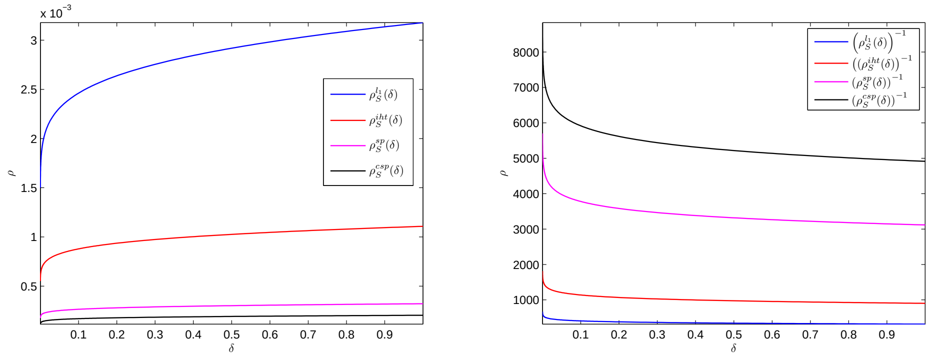

Figure 2.8: *Left panel:* The lower bounds on the strong exact recovery phase transition for Gaussian random matrices for the algorithms: $\ell_1$-minimization (Theorem 2.5.6), Iterative Hard Thresholding (Theorem 2.5.5), Subspace Pursuit (Theorem 2.5.4), and CoSaMP (Theorem 2.5.3). *Right panel:* The inverse of the phase transition lower bounds.

Lower bounds on the phase transitions $\rho_S^{alg}$ can also serve as proportionality constants with which we can determine the minimum number of measurement, $n$, proportional $k$, i.e. $n > \left(\rho_S^{alg}\right)^{-1} k$. The right panel of Figure 2.8 portrays the inverse of the lower bounds on the phase transition. For the different algorithms analysed above we can read off from the inverse plots in the left panel of Figure 2.8 the minimum number of measurements required using RIC$_2$ to guarantee exact reconstruction of all $k$-sparse vectors. The greedy algorithms, CoSaMP needs $n > 4913k$, SP needs $n > 3116k$, and IHT needs $n > 902k$; while $\ell_1$-minimization requires $n > 314k$. These curves are approximately $0.5 - 1\%$ higher than when our bounds are replaced by those of [19], see Figure 1 in [20]. Figure 2.9 shows a superimposition of the curves derived using the BCT bounds on the curves in Figure 2.8 based on our bounds. With the BCT bounds the minimum $n$ becomes $n > 4923k$ for CoSaMP, $n > 3124k$ for SP, $n > 907k$ for IHT, and $n > 317k$ for $\ell_1$-minimization.

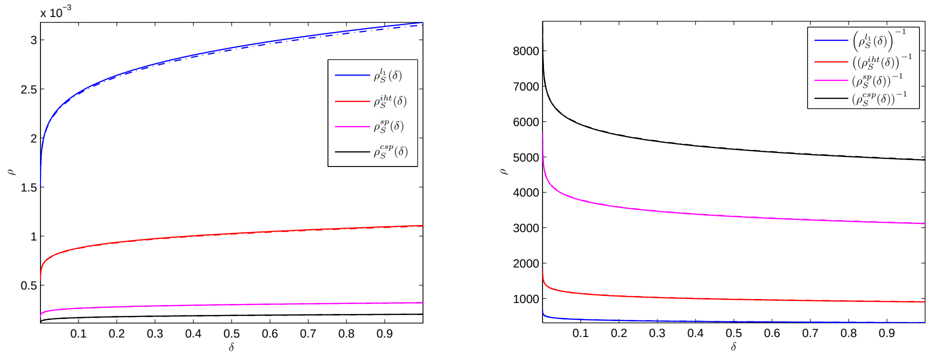

Figure 2.9: A superimposition of the curves from BCT (in dotted lines) on ours (in solid lines): *Left panel:* The lower bounds on the strong exact recovery phase transition for Gaussian random matrices for the algorithms: $\ell_1$-minimization (Theorem 2.5.6), Iterative Hard Thresholding (Theorem 2.5.5), Subspace Pursuit (Theorem 2.5.4), and CoSaMP (Theorem 2.5.3). *Right panel:* The inverse of the phase transition lower bounds.

In essence, the RIC$_2$ bounds for the Gaussian ensemble discussed here allow one to state values of $(k,n,N)$ when sparse approximation recovery conditions are satisfied, and from these, guarantee the recovery of $k$-sparse vectors from $(A,y)$. Unfortunately, all existing sparse approximation bound on the RIC$_2$ are sufficiently small that they are only satisfied for $\rho \ll 1$, typically on the order of $10^{-3}$. Although the bounds presented here are a strict improvement over the previously best known bounds, and for some $(\delta,\rho)$ achieve as much as a 20% decrease, see Figure 2.5, the improvements for $\rho \ll 1$ are meagre, approximately $0.5-1\%$. This limited improvement for compressed sensing algorithms is in large part due to the previous bounds being within 30% of empirically observed lower bounds on RIC$_2$ for $n = 400$ when $\rho < 10^{-2}$ [19].

## 2.6 Proofs

Here we present the proofs of the key theorems and lemmas stated in the chapter.

### 2.6.1 Lemma 2.3.5

We start by showing that $\lambda^{\max}(\delta,\rho;\gamma)$ has a unique minimum for each fixed $\delta,\rho$ and $\gamma \in [\rho,\delta^{-1}]$. Equation (2.8) gives the implicit relation between $\lambda^{\max}$ and $\gamma$ as

$$\delta\psi_{\max}\left(\lambda^{\max},\gamma\right) + \mathrm{H}(\rho\delta) - \delta\gamma\mathrm{H}\left(\rho/\gamma\right) = 0, \quad for\ \lambda^{\max} \geq 1+\gamma,$$

where

$$\psi_{\max}(\lambda^{\max},\gamma) = \frac{1}{2}\big[\,(1+\gamma)\ln\left(\lambda^{\max}\right) - \gamma\ln\gamma + 1 + \gamma - \lambda^{\max}\big].$$

Therefore, $\dfrac{d}{d\gamma}\left(\lambda^{\max}\right) = \dfrac{\lambda^{\max}}{\lambda^{\max}-(1+\gamma)}\ln\left[\dfrac{\lambda^{\max}\cdot(\gamma-\rho)^2}{\gamma^3}\right]$ is equal to zero when

$$\lambda^{\max}\cdot(\gamma-\rho)^2 = \gamma^3. \tag{2.19}$$

Let $\gamma_{\min}$ satisfy (2.19). Since $\lambda^{\max} \geq 1+\gamma > 0$, $\frac{d}{d\gamma}\left(\lambda^{\max}\right)$ is negative for $\gamma \in [\rho,\gamma_{\min})$, is zero at $\gamma_{\min}$ and is positive for $\gamma \in (\gamma_{\min},\delta^{-1})$, equation (2.8) has a unique minimum over $\gamma \in [\rho,\delta^{-1}]$, and the $\gamma$ that obtains the minimum is strictly greater than $\rho$.

Similarly, we show that $\lambda^{\min}(\delta,\rho;\gamma)$ has a unique maximum for each fixed $\delta,\rho$ and $\gamma \in [\rho,\delta^{-1}]$. Equation (2.7) gives the implicit relation between $\lambda^{\min}$ and $\gamma$ as

$$\delta\psi_{\min}\left(\lambda^{\min},\gamma\right) + \mathrm{H}(\rho\delta) - \delta\gamma\mathrm{H}\left(\rho/\gamma\right) = 0, \quad for\ \lambda^{\min} \leq 1-\gamma,$$

where

$$\psi_{\min}\left(\lambda^{\min},\gamma\right) := \mathrm{H}\left(\gamma\right) + \frac{1}{2}\Big[(1-\gamma)\ln\left(\lambda^{\min}\right) + \gamma\ln\gamma + 1 - \gamma - \lambda^{\min}\Big].$$

Therefore, $\frac{d}{d\gamma}\left(\lambda^{\min}\right) = \frac{\lambda^{\min}}{(1-\gamma)-\lambda^{\min}} \ln\left[\frac{\gamma^3 \cdot \lambda^{\min}}{(1-\gamma)^2 \cdot (\gamma-\rho)^2}\right]$ is equal to zero when

$$\gamma^3 \cdot \lambda^{\min} = (1-\gamma)^2(\gamma-\rho)^2. \tag{2.20}$$

Let $\gamma_{\max}$ satisfy (2.20). Since $0 < \lambda^{\min} \leq 1+\gamma$, $\frac{d}{d\gamma}\left(\lambda^{\min}\right)$ is positive for $\gamma \in [\rho, \gamma_{\max})$, zero at $\gamma_{\max}$ and negative for $\gamma \in (\gamma_{\max}, \delta^{-1})$, equation (2.7) has a unique maximum over $\gamma \in [\rho, \delta^{-1}]$, and the $\gamma$ that obtains the maximum is strictly greater than $\rho$. □

### 2.6.2 Theorem 2.3.2 and Propositions 2.4.1 and 2.4.2

Here we give a proof similar to that in [19] but we take great care with the non-exponential terms necessary for the calculation of bounds on probabilities for finite values of $(k, n, N)$ in Section 2.4. We present the proof for $\mathcal{U}^{BT}(\delta,\rho)$ in detail and sketch the proof of $\mathcal{L}^{BT}(\delta,\rho)$, that follows similarly.

The following lemma regarding the bound on the probability distribution function of the maximum eigenvalue of a Wishart matrix due to Edelman [62] is central to our proof. This is the same as Lemma 1.2.13 in Section 1.2.2. We restate it in the following lemma [62], presented in this form in [19] where they used the notation $f_{\max}(m,n;\lambda)$ for $f_{\lambda^{\max}}(x)$ in Lemma 1.2.13.

**Lemma 2.6.1.** *([62], presented in this form in [19]) Let $A_M$ be a matrix of size $n \times m$ whose entries are drawn i.i.d. from $\mathcal{N}(0, 1/n)$. Let $f_{\max}(m,n;\lambda)$ denote the distribution function for the largest eigenvalue of the derived Wishart matrix $A_M^* A_M$, of size $m \times m$. Then $f_{\max}(m,n;\lambda)$ satisfies*

$$f_{\max}(m,n;\lambda) \leq \left[(2\pi)^{\frac{1}{2}}(n\lambda)^{-\frac{3}{2}}\left(\frac{n\lambda}{2}\right)^{\frac{n+m}{2}} \frac{1}{\Gamma\left(\frac{m}{2}\right)\Gamma\left(\frac{n}{2}\right)}\right] e^{-\frac{n\lambda}{2}} =: g_{\max}(m,n;\lambda). \tag{2.21}$$

It is helpful at this stage to rewrite Lemma 2.6.1, separating the exponential and polynomial parts (with respect to $n$) of $g_{\max}(m,n;\lambda)$ as follows.

**Lemma 2.6.2.** *Let $\gamma_n = m/n \in [\rho_n, \delta_n^{-1}]$ and define $\psi_{\max}(\lambda,\gamma)$ as in (2.3). Then*

$$f_{\max}(m,n;\lambda) \leq g_{\max}(m,n;\lambda) \leq p_{\max}(n,\lambda;\gamma) \exp\left(n \cdot \psi_{\max}(\lambda,\gamma)\right), \tag{2.22}$$

*where $p_{\max}(n,\lambda;\gamma)$ is a polynomial in $n$, $\lambda$ and $\gamma$*

$$p_{\max}(n,\lambda;\gamma) = \left(\frac{8}{\pi}\right)^{1/2} \gamma^{-1} n^{-7/2} \lambda^{-3/2}. \tag{2.23}$$

*Proof.* Let $\gamma_n = \frac{m}{n}$ and $\frac{1}{n}\ln[g_{\max}(m,n;\lambda)] = \Phi_1(m,n;\lambda) + \Phi_2(m,n;\lambda) + \Phi_3(m,n;\lambda)$, where

$$\Phi_1(m,n;\lambda) = \frac{1}{2n}\ln(2\pi) - \frac{3}{2n}\ln(n\lambda), \quad \Phi_2(m,n;\lambda) = \frac{1}{2}\Big[(1+\gamma)\ln(\frac{n\lambda}{2}) - \lambda\Big]$$
$$\text{and} \quad \Phi_3(m,n;\lambda) = -\frac{1}{n}\ln\left(\Gamma\left(\frac{m}{2}\right)\Gamma\left(\frac{n}{2}\right)\right).$$

We simplify $\Phi_3(m,n;\lambda)$ by using the second Binet's log gamma formula [145]

$$\ln(\Gamma(z)) \geq (z - 1/2)\ln z - z + \ln\sqrt{2\pi}. \tag{2.24}$$

Thus we have

$$\Phi_2(m,n;\lambda) + \Phi_3(m,n;\lambda) \leq \frac{1}{2}\Big[(1+\gamma_n)\ln\lambda - \gamma_n\ln\gamma_n + 1 + \gamma_n - \lambda\Big] - n^{-1}\ln\left(\pi\gamma_n n^2/2\right).$$

Incorporating $\Phi_1(m,n;\lambda)$ and $-n^{-1}\ln\left(\pi\gamma_n n^2/2\right)$ into $p_{\max}(n,\lambda;\gamma)$ and defining the exponent (2.3) as

$$\psi_{\max}(\lambda,\gamma) := \lim_{n\to\infty}\frac{1}{n}\ln\left(g_{\max}(m,n;\lambda)\right) = \frac{1}{2}\Big[(1+\gamma)\ln\lambda - \gamma\ln\gamma + \gamma + 1 - \lambda\Big]$$

completes the proof. □

The upper RIC$_2$ bound $\mathcal{U}^{BT}(\delta,\rho)$ is obtained by constructing the groups $\mathcal{G}_i$ according to Lemma 2.3.3, taking a union bound over all $u = rN$ groups, and bounding the extreme eigenvalues within a group by the extreme eigenvalues of the Wishart matrices $A_{M_i}^*A_{M_i}$, see (2.12). In preparation for bounding the right-hand side of (2.12) we compute a bound on $rNg_{\max}(m,n;\lambda)$.

From Lemma 2.6.2 and equation (2.11) we have

$$2\lambda N\binom{N}{k}\binom{m}{k}^{-1} g_{\max}(m,n;\lambda) \leq p'_{\max}(n,\lambda)e^{n\psi_U(\lambda,\gamma)}, \tag{2.25}$$

where as in (2.15)

$$\psi_U(\lambda,\gamma) := \delta^{-1}\left[\mathrm{H}(\rho\delta) - \delta\gamma\mathrm{H}\left(\frac{\rho}{\gamma}\right) + \delta\psi_{\max}(\lambda,\gamma)\right]$$

and as in (2.14)

$$p'_{\max}(n,\lambda) := 2\lambda\left(\frac{5}{4}\right)^3\left(\frac{nN(\gamma-\rho)}{\gamma\delta(1-\rho\delta)}\right)^{1/2} p_{\max}(n,\lambda;\gamma).$$

The proof of proposition 2.4.1 then follows.

*Proof.* (Proof of Proposition 2.4.1)

For $\epsilon > 0$ with $\lambda^{\max}(\delta,\rho) = \min_{\gamma} \lambda^{\max}(\delta,\rho;\gamma)$ being the optimal solution to (2.8),

$$\begin{aligned}
\text{Prob}\left(U(k,n,N;A) > U(\delta_n,\rho_n)+\epsilon\right) &= \text{Prob}\left(U(k,n,N;A) > \lambda^{\max}(\delta_n,\rho_n) - 1 + \epsilon\right)\\
&= \text{Prob}\left(1+U(k,n,N;A) > \lambda^{\max}(\delta_n,\rho_n) + \epsilon\right)\\
&= N\binom{N}{k}\binom{m}{k}^{-1}\int_{\lambda^{\max}(\delta_n,\rho_n)+\epsilon}^{\infty} f_{\max}(m,n;\lambda)d\lambda\\
&\leq N\binom{N}{k}\binom{m}{k}^{-1}\int_{\lambda^{\max}(\delta_n,\rho_n)+\epsilon}^{\infty} g_{\max}(m,n;\lambda)d\lambda. \quad (2.26)
\end{aligned}$$

To bound the final integral in (2.26) we write $g_{\max}(m,n;\lambda)$ as a product of two separate functions, one of $\lambda$ and another of $n$ and $\gamma_n$, as $g_{\max}(m,n;\lambda) = \varphi(n,\gamma_n)\lambda^{-\frac{3}{2}}\lambda^{\frac{n}{2}(1+\gamma_n)}e^{-\frac{n}{2}\lambda}$ where

$$\varphi(n,\gamma_n) = (2\pi)^{\frac{1}{2}}(n)^{-\frac{3}{2}}\left(\frac{n}{2}\right)^{\frac{n}{2}(1+\gamma_n)}\frac{1}{\Gamma\left(\frac{n}{2}\gamma_n\right)\Gamma\left(\frac{n}{2}\right)}.$$

With this and using the fact that $\lambda^{\max}(\delta_n,\rho_n) > 1+\gamma_n$ and that $\lambda^{\frac{n}{2}(1+\gamma_n)}e^{-\frac{n}{2}\lambda}$ is strictly decreasing in $\lambda$ on $[\lambda^{\max}(\delta_n,\rho_n),\infty)$ we can bound the integral in (2.26) as follows:

$$\begin{aligned}
&\int_{\lambda^{\max}(\delta_n,\rho_n)+\epsilon}^{\infty} g_{\max}(m,n;\lambda)d\lambda\\
&\leq \varphi(n,\gamma_n)[\lambda^{\max}(\delta_n,\rho_n)+\epsilon]^{\frac{n}{2}(1+\gamma_n)}e^{-\frac{n}{2}(\lambda^{\max}(\delta_n,\rho_n)+\epsilon)}\int_{\lambda^{\max}(\delta_n,\rho_n)+\epsilon}^{\infty}\lambda^{-\frac{3}{2}}d\lambda\\
&= [\lambda^{\max}(\delta_n,\rho_n)]^{\frac{3}{2}}g_{\max}\big[m,n;\lambda^{\max}(\delta_n,\rho_n)+\epsilon\big]\int_{\lambda^{\max}(\delta_n,\rho_n)+\epsilon}^{\infty}\lambda^{-\frac{3}{2}}d\lambda\\
&= 2\lambda^{\max}(\delta_n,\rho_n)g_{\max}\big[m,n;\lambda^{\max}(\delta_n,\rho_n)+\epsilon\big]. \quad (2.27)
\end{aligned}$$

Thus (2.26) and (2.27) together give a bound on $\text{Prob}\left(U(k,n,N;A) > U(\delta_n,\rho_n)+\epsilon\right)$ as

$$\begin{aligned}
&2\lambda^{\max}(\delta_n,\rho_n)rNg_{\max}\big[m,n;\lambda^{\max}(\delta_n,\rho_n)+\epsilon\big],\\
&\leq p'_{\max}\left(n,\lambda^{\max}(\delta_n,\rho_n)\right)\exp\left[n\cdot\psi_U\left(\lambda^{\max}(\delta_n,\rho_n)+\epsilon\right)\right]\\
&\leq p'_{\max}\left(n,\lambda^{\max}(\delta_n,\rho_n)\right)\exp\left[n\epsilon\cdot\frac{d}{d\lambda}\psi_U\left(\lambda^{\max}(\delta_n,\rho_n)\right)\right], \quad (2.28)
\end{aligned}$$

where $r = \binom{N}{k}\binom{m}{k}^{-1}$, and the last inequality is due to $\psi_U(\lambda)$ being strictly concave. □

The following is a corollary to Proposition 2.4.1.

**Corollary 2.6.3.** *Let* $(\delta,\rho) \in (0,1)^2$ *and let* $A$ *be a matrix of size* $n \times N$ *whose entries are drawn i.i.d. from* $\mathcal{N}(0,1/n)$*. Define* $\mathcal{U}^{BT}(\delta,\rho) = \lambda^{\max}(\delta,\rho)-1$ *where* $\lambda^{\max}(\delta,\rho;\gamma)$ *is the solution of (2.8) for each* $\gamma \in [\rho,\delta^{-1}]$ *and* $\lambda^{\max}(\delta,\rho) := \min_{\gamma}\lambda^{\max}(\delta,\rho;\gamma)$*. Then for any* $\epsilon > 0$*, in the* *proportional-growth asymptotics*

$$Prob\big(U(k,n,N;A) > \mathcal{U}^{BT}(\delta,\rho) + \epsilon\big) \to 0$$

*exponentially in $n$.*

*Proof.* From (2.28), since $\frac{d}{d\lambda}\psi_U\left(\lambda^{\max}(\delta_n,\rho_n)\right) < 0$ is strictly bounded away from zero and all the limits of $(\delta_n,\rho_n)$ are smoothly varying functions, we conclude for any $\epsilon > 0$

$$\lim_{n\to\infty} \text{Prob}\big(U(k,n,N;A) > \mathcal{U}^{BT}(\delta,\rho) + \epsilon\big) \to 0.$$

□

Thus we finish the proof for $\mathcal{U}^{BT}(\delta,\rho)$. We sketch the similar proof for Proposition 2.4.2 and $\mathcal{L}^{BT}(\delta,\rho)$. Bounds on the probability distribution function of the minimum eigenvalue of a Wishart matrix are given by Lemma 1.2.12 in Section 1.2.2. We restate it in the following lemma [62], presented in this form in [19] where they used the notation $f_{\min}(m,n;\lambda)$ for $f_{\lambda^{\min}}(x)$ in Lemma 1.2.12.

**Lemma 2.6.4.** *Let $A_M$ be a matrix of size $n \times m$ whose entries are drawn i.i.d. from $\mathcal{N}(0,1/n)$. Let $f_{\min}(m,n;\lambda)$ denote the distribution function for the smallest eigenvalue of the derived Wishart matrix $A_M^* A_M$, of size $m \times m$. Then $f_{\min}(m,n;\lambda)$ satisfies*

$$f_{\min}(m,n;\lambda) \le (\frac{\pi}{2n\lambda})^{\frac{1}{2}}\left(\frac{n\lambda}{2}\right)^{\frac{n-m}{2}}\left[\frac{\Gamma\left(\frac{n+1}{2}\right)}{\Gamma\left(\frac{m}{2}\right)\Gamma\left(\frac{n-m+1}{2}\right)\Gamma\left(\frac{n-m+2}{2}\right)}\right]e^{-\frac{n\lambda}{2}} =: g_{\min}(m,n;\lambda).$$

Again an explicit expression of $f_{\min}(m,n;\lambda)$ in terms of exponential and polynomial parts leads to the following Lemma.

**Lemma 2.6.5.** *Let $\gamma_n = m/n$ and define $\psi_{\min}(\lambda,\gamma)$ as in (2.2). Then*

$$f_{\min}(m,n;\lambda) \le g_{\min}(m,n;\lambda) \le p_{\min}(n,\lambda)\exp\left(n\cdot\psi_{\min}(\lambda,\gamma)\right),$$

*where $p_{\min}(n,\lambda;\gamma)$ is a polynomial in $n,\lambda$ and $\gamma$, given by*

$$p_{\min}(n,\lambda;\gamma) = \frac{e}{2\pi\sqrt{2\lambda}}.$$

The proof of Lemma 2.6.5 follows that of Lemma 2.6.2 and is omitted for brevity. Equipped with Lemma 2.6.5 a large deviation analysis yields

$$2\lambda N\binom{N}{k}\binom{m}{k}^{-1} g_{\min}(m,n;\lambda) \le p'_{\min}(n,\lambda)e^{n\psi_L(\lambda,\gamma)}, \tag{2.29}$$

where as in (2.18)

$$\psi_L(\lambda,\gamma) := \delta^{-1}\left[\mathrm{H}(\rho\delta) - \delta\gamma\mathrm{H}\left(\frac{\rho}{\gamma}\right) + \delta\psi_{\min}(\lambda,\gamma)\right]$$

and as in (2.17)

$$p'_{\min}(n,\lambda) := 2\lambda\left(\frac{5}{4}\right)^3\left(\frac{nN(\gamma-\rho)}{\gamma\delta(1-\rho\delta)}\right)^{1/2} p_{\min}(n,\lambda).$$

With Lemma 2.6.5 and (2.29), Proposition 2.4.2 follows similarly to the proof of Proposition 2.4.1 stated earlier in this section. The bound $\mathcal{L}^{BT}(\delta,\rho)$ is a corollary of Proposition 2.4.2.

**Corollary 2.6.6.** *Let $(\delta,\rho) \in (0,1)^2$ and let $A$ be a matrix of size $n \times N$ whose entries are drawn i.i.d. from $\mathcal{N}(0,1/n)$. Define $\mathcal{L}^{BT}(\delta,\rho) := 1-\lambda_{\min}(\delta,\rho)$, where $\lambda_{\min}(\delta,\rho;\gamma)$ is the solution of (2.7) for each $\gamma \in [\rho,\delta^{-1}]$ and $\lambda^{\min}(\delta,\rho) := \min_{\gamma} \lambda^{\min}(\delta,\rho;\gamma)$. Then for any $\epsilon > 0$, in the proportional-growth asymptotic*

$$Prob\left(L(k,n,N;A) > \mathcal{L}^{BT}(\delta,\rho) + \epsilon\right) \to 0$$

*exponentially in $n$.* □

# Chapter 3

# Asymptotic Expansion of $\mathrm{RIC}_2$ for Gaussian Matrices

## 3.1 Introduction

In Chapter 2 we showed that$\mathrm{RIC}_2$ bounds for Gaussian matrices have been derived [6, 19, 33] focusing on the linear growth asymptotics given by Definition 2.1.1, i.e. limits $k/n \to \rho \in (0,1)$ and $n/N \to \delta \in (0,1)$ as $(k,n,N) \to \infty$, see Theorems 2.2.2, 2.2.4 and 2.3.2. Unfortunately, these bounds are given in terms of implicitly defined functions, see Definitions 2.2.3 and 2.3.1, obscuring their dependence on $\rho$ and $\delta$.

Here, we present simple expressions which bound the $\mathrm{RIC}_2$ of Gaussian matrices in three asymptotic settings: (a) $\delta \in (0,1)$ and $\rho \ll 1$ where the $\mathrm{RIC}_2$ converge to zero as $\rho$ approaches zero, (b) $\rho \in (0,1)$ and $\delta \ll 1$ where the upper $\mathrm{RIC}_2$ become unbounded and the lower $\mathrm{RIC}_2$ converges to its bound of one as $\delta$ approaches zero, and (c) along the path $\rho_\gamma(\delta) = \frac{1}{\gamma \log(\delta^{-1})}$ for $\delta \ll 1$ where the $\mathrm{RIC}_2$ approach a nonzero constant as $\delta$ approaches zero.

The Chapter [1] is outlined as follows. In Section 3.2 we present the asymptotic formulae for the bounds and in Section 3.3 we discuss the implication of these formulae to CS. We demonstrate the accuracy of the formulae in Section 3.4 and in Section 3.5 we prove CS corollaries presented in Section 3.3. We conclude the chapter with the proofs of the main results, Theorems 3.2.1 - 3.2.3 and Corollary 3.2.4, in Section 3.6.

## 3.2 Asymptotic Formulae for $\mathrm{RIC}_2$ Bounds

The bounds presented here build on the results in [19] and are specific to Gaussian matrices, carefully balancing combinatorial quantities with the tail behaviour of the largest and smallest

[1] Material in this chapter has been prepared for publication and in preprint [7] in a joint authorship with J. Tanner whose permission has been obtained for the inclusion of the material.

singular values of Gaussian matrices. The specificity of these bounds to Gaussian matrices gives great accuracy than what subgaussian tail bounds provide [12]. A similar analysis could be conducted for the subgaussian case by considering the bounds in [39] stated for the Gaussian case, but which are equally valid for the subgaussian case. For brevity we do not consider the subgaussian case here.

In the analysis that follow we use Theorem 2.2.4 and Definition 2.2.3 from the BCT bounds in Chapter 2. We used the BCT bounds because in these types of values of $\delta$ and $\rho$ they are easier to compute than our (BT) bounds and the fact is, in these regime of $\delta$ and $\rho$, our bounds are the same as the BCT bounds. Note that in Definition 2.2.3 we have the upper RIC$_2$ bound defined as $\mathcal{U}(\delta,\rho) := \min_{\nu\in[\rho,1]} \lambda^{\max}(\delta,\nu)-1$, without the superscript and subscript BCT. Due to the overestimation that occurs when $\delta\rho \approx 1/2$ the minimum occurs at $\nu \in (\rho, 1]$. In the range of values of $\delta$ and $\rho$ considered here we will always have the minimum occurring at $\nu = \rho$ hence $\mathcal{U}(\delta,\rho) := \lambda^{\max}(\delta,\rho)-1$, which is what we use in the ensuing derivations.

Theorem 2.2.4 states that, for $k$, $n$, and $N$ large, it is unlikely that the RIC$_2$ exceed the constants $\mathcal{L}(\delta,\rho)$ and $\mathcal{U}(\delta,\rho)$ by more than any $\epsilon$. In the limit where $n/N = \delta_n \to \delta \in (0,1)$ and $k/n = \rho_n \to \rho \ll 1$, the RIC$_2$ converge to zero, causing the resulting bounds to become vacuous. Theorem 3.2.1 states the dominant terms in the bounds, and that the true RIC$_2$ are unlikely to exceed these bounds by a multiplicative factor $(1+\epsilon)$ for any $\epsilon > 0$. The dominant terms can be contrasted with $2\sqrt{\rho}+\rho$ which is the deviation from one of the expected value of the extreme eigenvalues of a Wishart matrix stated in Lemma 1.2.16 in Chapter 1.

Each of Theorems 3.2.1 – 3.2.3 state that the probability under consideration *converge exponentially* to 1 in $k$ or $n$ which we use as a shorthand for saying one minus the probability considered being bounded by a function decaying exponentially to zero in the variable stated; the explicit bound is given in the proof of the theorem. An implication of Theorem 3.2.1 for the compressed sensing algorithm, Orthogonal Matching Pursuit (OMP), is given in Corollary 3.3.2; while an implication of Theorem 3.2.3 for other compressed sensing algorithms is given in Corollary 3.3.1.

**Theorem 3.2.1** (Gaussian RIC$_2$ Bounds: $\rho \ll 1$). *Let $\widetilde{\mathcal{U}}^{\rho}(\delta,\rho)$ and $\widetilde{\mathcal{L}}^{\rho}(\delta,\rho)$ be defined as*

$$\widetilde{\mathcal{L}}^{\rho}(\delta,\rho) = \widetilde{\mathcal{U}}^{\rho}(\delta,\rho) = \sqrt{2\rho\log\left(\frac{1}{\delta^2\rho^3}\right)+c\rho}. \tag{3.1}$$

*Fix $\epsilon > 0$ and $c > 6$. For each $\delta \in (0,1)$ there exists a $\rho_0 > 0$ such that in the limit where $\frac{n}{N} \to \delta$, $\frac{k}{n} \to \rho \in (0,\rho_0)$, and $\frac{\log n}{k} \to 0$ as $k \to \infty$, sample each $n \times N$ matrix $A$ from the Gaussian ensemble, $\mathcal{N}\left(0,\frac{1}{n}\right)$, then*

$$Prob\Big(L(k,n,N;A) < (1+\epsilon)\widetilde{\mathcal{L}}^{\rho}(\delta,\rho)\Big) \to 1 \quad \& \quad Prob\Big(U(k,n,N;A) < (1+\epsilon)\widetilde{\mathcal{U}}^{\rho}(\delta,\rho)\Big) \to 1$$

*exponentially in $k$.*

Theorem 3.2.2 considers a limiting case where the upper RIC$_2$ diverges and the lower RIC$_2$ converges to its bound of one. With $L(k,n,N;A)$ converging to one, it is bounded by an arbitrarily small multiplicative constant, whereas $U(k,n,N;A)$ is bounded by an additive constant.

**Theorem 3.2.2** (Gaussian RIC$_2$ Bounds: $\delta \ll 1$). *Let $\widetilde{\mathcal{U}}^\delta(\delta,\rho)$ and $\widetilde{\mathcal{L}}^\delta(\delta,\rho)$ be defined as*

$$\widetilde{\mathcal{U}}^\delta(\delta,\rho) = \rho\log\left(\frac{1}{\delta^2\rho^3}\right) + (1+\rho)\log\left[c\log\left(\frac{1}{\delta^2\rho^3}\right)\right] + 3\rho, \tag{3.2}$$

$$\widetilde{\mathcal{L}}^\delta(\delta,\rho) = 1 - \exp\left(-\frac{3\rho+c}{1-\rho}\right)\cdot\left(\delta^2\rho^3\right)^{\frac{\rho}{1-\rho}}. \tag{3.3}$$

*Fix $\epsilon > 0$ and $c > 1$. For each $\rho \in (0,1)$ there exists a $\delta_0 > 0$ such that in the limit where $\frac{k}{n} \to \rho$, $\frac{n}{N} \to \delta \in (0,\delta_0)$ as $n \to \infty$, sample each $n \times N$ matrix $A$ from the Gaussian ensemble, $\mathcal{N}\left(0,\frac{1}{n}\right)$, then*

$$\text{Prob}\left(L(k,n,N;A) < (1+\epsilon)\widetilde{\mathcal{L}}^\delta\left(\delta,\rho\right)\right) \to 1 \quad \text{and} \quad \text{Prob}\left(U(k,n,N;A) < \widetilde{\mathcal{U}}^\delta\left(\delta,\rho\right)+\epsilon\right) \to 1$$

*exponentially in $n$.*

Theorem 3.2.3 considers the path in which both $\rho_n$ and $\delta_n$ converge to zero, but in such a way that the RIC$_2$ approach nonzero constants. This path is of particular interest in applications where RIC$_2$ are required to remain bounded, but where the most extreme advantages of the method are achieved for one of the quantities approaching zero. For example, compressed sensing achieves increased gains in undersampling as $\delta_n$ decreases to zero; however, all compressed sensing algorithmic guarantees involving RIC$_2$ require the RIC$_2$ to remain bounded. The limit considered in Theorem 3.2.3 provides explicit formula for these algorithms in the case where the undersampling is greatest, see Corollary 3.3.1.

**Theorem 3.2.3** (Gaussian RIC$_2$ Bounds: $\rho_n \to (\gamma\log(1/\delta_n))^{-1}$ and $\delta \ll 1$). *Consider that we let $\rho_\gamma(\delta) = \frac{1}{\gamma\log(\delta^{-1})}$ and $\widetilde{\mathcal{U}}^\gamma\left(\delta,\rho_\gamma(\delta)\right)$ and $\widetilde{\mathcal{L}}^\gamma\left(\delta,\rho_\gamma(\delta)\right)$ are defined as*

$$\widetilde{\mathcal{U}}^\gamma\left(\delta,\rho_\gamma(\delta)\right) = \sqrt{2\rho_\gamma(\delta)\log\left(\frac{1}{\delta^2\rho_\gamma^3(\delta)}\right) + 6\rho_\gamma(\delta)} + c_u\left[2\rho_\gamma(\delta)\log\left(\frac{1}{\delta^2\rho_\gamma^3(\delta)}\right) + 6\rho_\gamma(\delta)\right] \tag{3.4}$$

$$\widetilde{\mathcal{L}}^\gamma\left(\delta,\rho_\gamma(\delta)\right) = \sqrt{2\rho_\gamma(\delta)\log\left(\frac{1}{\delta^2\rho_\gamma^3(\delta)}\right) + 6\rho_\gamma(\delta)} - c_l\left[\rho_\gamma(\delta)\log\left(\frac{1}{\delta^2\rho_\gamma^3(\delta)}\right) + 6\rho_\gamma(\delta)\right]. \tag{3.5}$$

*Fix $\gamma > \gamma_0$ (which $\gamma_0 \geq 4$), $\epsilon > 0$, $c_u > 1/3$ and $c_l < 1/3$. There exists a $\delta_0 > 0$ such that in the limit where $\frac{k}{n} \to \rho_\gamma(\delta_0)$, $\frac{n}{N} \to \delta \in (0,\delta_0)$ as $n \to \infty$, sample each $n \times N$ matrix $A$ from the Gaussian ensemble, $\mathcal{N}\left(0,\frac{1}{n}\right)$, then*

$$\text{Prob}\left(L(k,n,N;A) < \widetilde{\mathcal{L}}^\gamma\left(\delta,\rho_\gamma(\delta)\right)+\epsilon\right) \to 1 \text{ and } \text{Prob}\left(U(k,n,N;A) < \widetilde{\mathcal{U}}^\gamma\left(\delta,\rho_\gamma(\delta)\right)+\epsilon\right) \to 1$$

*exponentially in $n$.*

Theorem 3.2.3 considers the path $\rho_\gamma(\delta)$ for $\delta \ll 1$; passing to the limit as $\delta \to 0$, the functions $\widetilde{\mathcal{U}}^\gamma(\delta, \rho_\gamma(\delta))$ and $\widetilde{\mathcal{L}}^\gamma(\delta, \rho_\gamma(\delta))$ defined as (3.4) and (3.5) converge to simple functions of $\gamma$.

**Corollary 3.2.4** (Gaussian RIC$_2$ Bounds: $\rho_n \to (\gamma \log(1/\delta_n))^{-1}$ as $\delta \to 0$)**.** *Consider that* $\widetilde{\mathcal{U}}^\gamma(\delta, \rho_\gamma(\delta))$ *and* $\widetilde{\mathcal{L}}^\gamma(\delta, \rho_\gamma(\delta))$ *are defined as in* (3.4) *and* (3.5)*, respectively, with* $\rho_\gamma(\delta) = \frac{1}{\gamma \log(\delta^{-1})}$*. Then*

$$\lim_{\delta \to 0} \widetilde{\mathcal{U}}^\gamma(\delta, \rho_\gamma(\delta)) = \frac{2}{\sqrt{\gamma}} + \frac{4}{\gamma} c_u \tag{3.6}$$

$$\lim_{\delta \to 0} \widetilde{\mathcal{L}}^\gamma(\delta, \rho_\gamma(\delta)) = \frac{2}{\sqrt{\gamma}} - \frac{4}{\gamma} c_l. \tag{3.7}$$

The accuracy of Theorems 3.2.1 - 3.2.3 and Corollary 3.2.4 are discussed in Section 3.4 and proven in Section 3.6.

## 3.3 Implications for Compressed Sensing

We remind the reader that the theory of compressed sensing has developed conditions in which a vector of interest $x$, or an approximation thereof, can be recovered. Most remarkably, for any fixed ratio $\frac{n}{N}$, the recovery guarantees achieve the optimal order of the number of measurements being proportional to the information content in $x$ ($n$ proportional to $k$), see Section 2.5.1. Furthermore, in compressed sensing the recovery algorithms remain effective for $\frac{k}{n}$ decaying slowly as the number of measurements becomes vanishingly small compared to the signal length, $\frac{n}{N} \to 0$. In fact, it is known that $\rho^{alg}(\delta)$ becomes proportional to $\frac{1}{\log(\delta^{-1})}$ as $\delta \to 0$. This constant of proportionality can be deduced from Theorem 3.2.3; the resulting sampling theorems for representative compressed sensing algorithms are stated in Corollary 3.3.1 for $c_u = c_l = 1/3$.

**Corollary 3.3.1.** *Given a sensing matrix, $A$, of size $n \times N$ whose entries are drawn i.i.d. from $\mathcal{N}(0, \frac{1}{n})$, in the limit as $\frac{n}{N} \to 0$ a sufficient condition for recovery for compressed sensing algorithms is $n \geq \gamma k \log\left(\frac{N}{n}\right)$ measurements with $\gamma = 37$ for $l_1$-minimization [37], $\gamma = 96$ for Iterative Hard Thresholding (IHT) [25], $\gamma = 279$ for Subspace Pursuit (SP) [50] and $\gamma = 424$ for Compressed Sampling Matching Pursuit (CoSaMP) [109].*

### Orthogonal Matching Pursuit (OMP)

Not all compressed sensing algorithms achieve the optimal order of $k$ being proportional to $n$. One such algorithm is Orthogonal Matching Pursuit (OMP) [143, 138], which has recently been analysed using RIC$_2$, see [106] and references therein. OMP like the earlier greedy algorithms discussed in Section 2.5.1, iteratively identifies the correct support set by adding one index to the support and updating the target vector $\hat{x}$ as the vector supported on the target support that best fits the measurements. Algorithm 4 of Table 3.1 is a pseudocode of OMP.

```
Input: $A,\ y,\ k$
Output: $k$-sparse approximation $\hat{x}$ of the target signal $x$
Initialization:
    Set $\Lambda^0 = \emptyset$
    Set $r^0 = y$
Iteration: During iteration $l$, do
    Find $\lambda^l = \arg\max_{j=1,\dots,N} |\langle r^{l-1}, a_j\rangle|$ where $a_j$ is the $j^{\text{th}}$ column of $A$
    Augment $\Lambda^l = \Lambda^{l-1} \cup \{\lambda^l\}$
    Solve $\tilde{x}^l = \arg\min_x \|y - A_{\Lambda^l} x\|_2$
    Calculate new approximation of data as $\tilde{y}^l = A_{\Lambda^l}\tilde{x}^l$, and new residual as $r^l = y - \tilde{y}^l$
    if $l = k$ then
        return $\hat{x}$ defined by $\hat{x}_{\{1,\dots,N\}\setminus\Lambda^l} = 0$ and $\hat{x}_{\Lambda^l} = \tilde{x}_{\Lambda^l}$
    else
        Perform iteration $l+1$
    end if
```

Table 3.1: **Algorithm 4** – Orthogonal Matching Pursuit (OMP) [143].

An analytic asymptotic sampling theorem for OMP can be deduced from Theorem 3.2.1, see Corollary 3.3.2.

**Corollary 3.3.2.** *Given a sensing matrix, $A$, of size $n \times N$ whose entries are drawn i.i.d. from $\mathcal{N}(0, \frac{1}{n})$, in the limit as $\frac{n}{N} \to \delta \in (0,1)$ a sufficient condition for recovery for Orthogonal Matching Pursuit (OMP) is*

$$n > 2k(k-1)[3 + 2\log N + \log n - 3\log k].$$

## 3.4 Accuracy of Main Results (Formulae)

This section discusses the accuracy of Theorems 3.2.1 - 3.2.3 and Corollary 3.2.4, comparing the expressions with the bounds in Theorem 2.2.4, which are defined [19] implicitly in Definition 2.2.3. Therefore, in the ensuing discussion on the accuracy of our results $\mathcal{U}(\delta,\rho) = \mathcal{U}^{BCT}(\delta,\rho)$ and $\mathcal{L}(\delta,\rho) = \mathcal{L}^{BCT}(\delta,\rho)$.

Theorems 3.2.1 - 3.2.3 are discussed in Sections 3.4.1 - 3.4.3 respectively. Each section includes plots illustrating the formulae and relative difference in the relevant regimes. The discussion of Corollary 3.2.4 is included in Section 3.4.3. This Section concludes with proofs of the compressed sensing sampling theorems discussed in Section 3.3.

### 3.4.1 Theorems 3.2.1: $\delta$ fixed and $\rho \ll 1$

Figure 3.1, left panel, displays the bounds $\mathcal{U}(\delta,\rho)$ and $\mathcal{L}(\delta,\rho)$ from Theorem 2.2.4 for $\delta = 0.25$, $c = 6$ and $\rho \in (10^{-10}, 10^{-1})$. This is the regime of Theorem 3.2.1 and the formula (3.1) is also displayed. Formula (3.1) is observed to accurately approximate $\mathcal{U}(\delta,\rho)$ and $\mathcal{L}(\delta,\rho)$ respectively in both an absolute and relative scale, in the left and right panel of Figure 3.1

respectively.

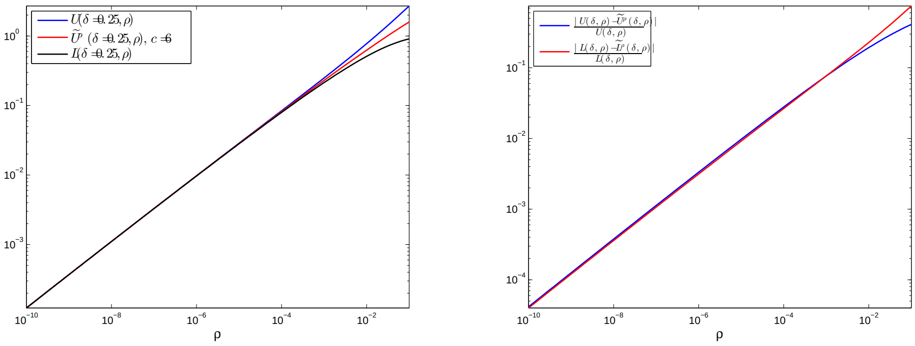

Figure 3.1: $\mathrm{RIC}_2$ bounds for $\delta = 0.25,\ c = 6$ and $\rho \in (10^{-10}, 10^{-1})$. *Left panel:* $\mathcal{U}(\delta,\rho)$, $\mathcal{L}(\delta,\rho)$, $\widetilde{\mathcal{U}}^{\rho}(\delta,\rho)$ and $\widetilde{\mathcal{L}}^{\rho}(\delta,\rho)$. *Right panel:* relative differences, $\frac{|\mathcal{U}(\delta,\rho)-\widetilde{\mathcal{U}}^{\rho}(\delta,\rho)|}{\mathcal{U}(\delta,\rho)}$ and $\frac{|\mathcal{L}(\delta,\rho)-\widetilde{\mathcal{L}}^{\rho}(\delta,\rho)|}{\mathcal{L}(\delta,\rho)}$.

### 3.4.2 Theorems 3.2.2: $\rho$ fixed and $\delta \ll 1$

Figure 3.2 displays the bounds $\mathcal{U}(\delta,\rho)$ and $\mathcal{L}(\delta,\rho)$ from Theorem 2.2.4 along with the formulae (3.2) and (3.3) of Theorem 3.2.2 in the left and right panels respectively; for diversity the upper $\mathrm{RIC}_2$ bound is shown for $\rho = 0.5$ and the lower $\mathrm{RIC}_2$ bound for $\rho = 0.1$, in both instances $\delta \in (10^{-50}, 10^{-1})$ and $c = 1$. This is the regime of $\rho$ fixed and $\delta \ll 1$ where the upper $\mathrm{RIC}_2$ diverges to infinity and the lower $\mathrm{RIC}_2$ converges to its trivial unit bound as $\delta$ approaches zero. The bounds of Theorem 3.2.2 are observed to accurately approximate $\mathcal{U}(\delta,\rho)$ and $\mathcal{L}(\delta,\rho)$ in both an absolute and relative scale, in Figure 3.2 and 3.3 respectively.

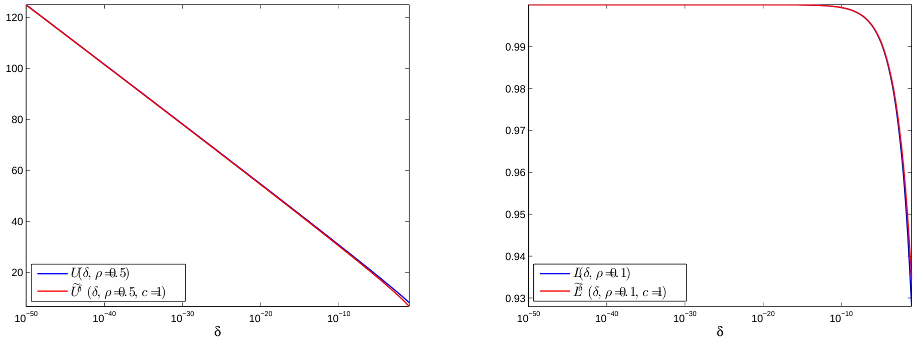

Figure 3.2: $\mathrm{RIC}_2$ bounds for $\delta \in (10^{-50}, 10^{-1})$ and $c = 1$. *Left panel:* $\mathcal{U}(\delta,\rho)$ and $\widetilde{\mathcal{U}}^{\delta}(\delta,\rho)$ for $\rho = 0.5$. *Right panel:* $\mathcal{L}(\delta,\rho)$ and $\widetilde{\mathcal{L}}^{\delta}(\delta,\rho)$ for $\rho = 0.1$.

### 3.4.3 Theorems 3.2.3: $\rho = (\gamma \log(1/\delta))^{-1}$ and $\delta \ll 1$

The left panel of Figure 3.4 displays the bounds $\mathcal{U}(\delta,\rho)$ and $\mathcal{L}(\delta,\rho)$ from Theorem 2.2.4 along with the formulae (3.4) and (3.5) of Theorem 3.2.3 for $c_u = c_l = 1/3$, $\gamma = 300$ and $\delta \in (10^{-80}, 10^{-1})$. The formulae of Theorem 3.2.3 are observed to accurately approximate the

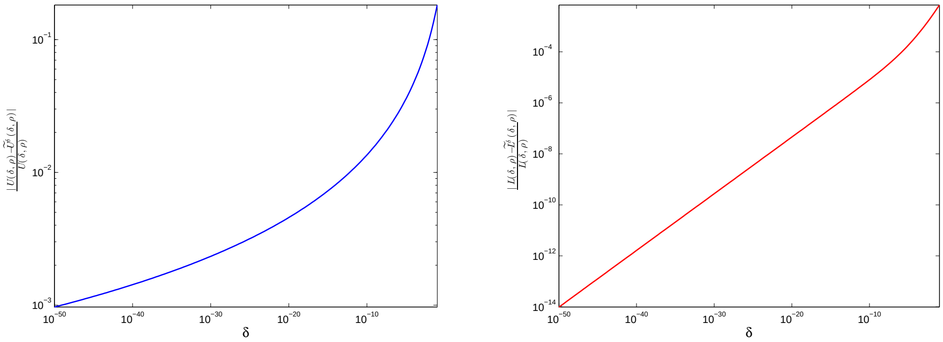

Figure 3.3: Relative difference in RIC$_2$ bounds for $\delta \in (10^{-50}, 10^{-1})$ and $c = 1$. *Left panel:* $\frac{|\mathcal{U}(\delta,\rho)-\widetilde{\mathcal{U}}^{\delta}(\delta,\rho)|}{\mathcal{U}(\delta,\rho)}$ for $\rho = 0.5$. *Right panel:* $\frac{|\mathcal{L}(\delta,\rho)-\widetilde{\mathcal{L}}^{\delta}(\delta,\rho)|}{\mathcal{L}(\delta,\rho)}$ for $\rho = 0.1$.

bounds in Theorem 2.2.4 over the entire range of $\delta$; the relative differences between these bounds are displayed in the right panel of Figure 3.4.

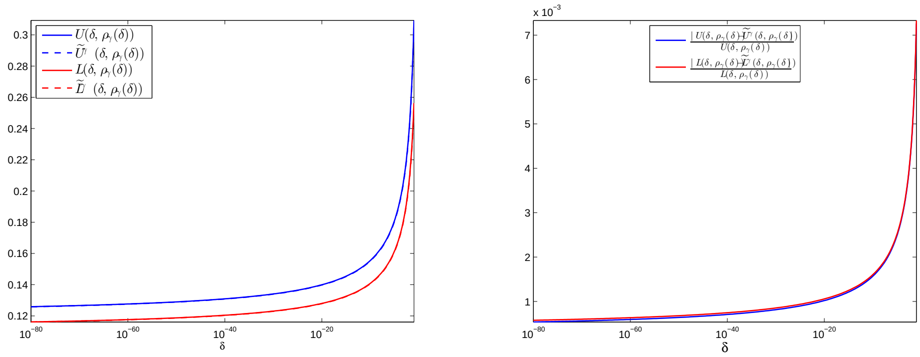

Figure 3.4: A comparison of $\widetilde{\mathcal{U}}^{\gamma}(\delta, \rho_\gamma(\delta))$ and $\widetilde{\mathcal{L}}^{\gamma}(\delta, \rho_\gamma(\delta))$ to $\mathcal{U}(\delta,\rho)$ and $\mathcal{L}(\delta,\rho)$ respectively for $c_u = c_l = 1/3$, $\gamma = 300$ and $\delta \in (10^{-80}, 10^{-1})$. *Left panel:* $\widetilde{\mathcal{U}}^{\gamma}(\delta, \rho_\gamma(\delta))$, $\mathcal{U}(\delta,\rho)$, $\widetilde{\mathcal{L}}^{\gamma}(\delta, \rho_\gamma(\delta))$, and $\widetilde{\mathcal{L}}^{\gamma}(\delta, \rho_\gamma(\delta))$. *Right panel:* their relative differences $\frac{|\mathcal{U}(\delta,\rho)-\widetilde{\mathcal{U}}^{\gamma}(\delta,\rho_\gamma(\delta))|}{\mathcal{U}(\delta,\rho)}$ and $\frac{|\mathcal{L}(\delta,\rho)-\widetilde{\mathcal{L}}^{\gamma}(\delta,\rho_\gamma(\delta))|}{\mathcal{L}(\delta,\rho)}$.

The left panel of Figure 3.4 shows the RIC$_2$ bounds converging to nonzero constants as $\delta$ approaches zero, displayed for $c_u = c_l = 1/3$ and $\gamma = 300$. Corollary 3.2.4 provides formula for $\delta \ll 1$, which is observed in Figure 3.5 to accurately approximate the formulae in Theorem 3.2.3 for $c_u = c_l = 1/3$ and $\delta = 10^{-80}$, uniformly over $\gamma \in (1, 300)$.

## 3.5 Proof of Compressed Sensing Corollaries

Corollaries 3.3.1 and 3.3.2 follow directly from Theorems 3.2.3 and 3.2.1 and existing RIC$_2$ based recovery guarantees for the associated algorithms in [20] and [106] respectively.

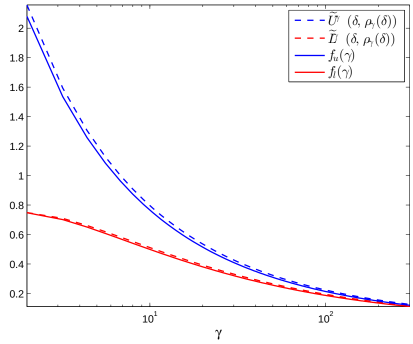

Figure 3.5: Plots of the $\widetilde{\mathfrak{U}}^{\gamma}(\delta, \rho_\gamma(\delta))$ and $\widetilde{\mathfrak{L}}^{\gamma}(\delta, \rho_\gamma(\delta))$ as well as $f_u(\gamma)$ and $f_l(\gamma)$ given by (3.6) and (3.7) respectively, for $c_u = c_l = 1/3$, $\delta = 10^{-80}$ and $\gamma \in (1, 300)$.

### 3.5.1 Proof of Corollary 3.3.1

*Proof.* There is an extensive literature on compressed sensing and sparse approximation algorithms which are guaranteed to recover vectors $\hat{x}$ that satisfy bounds of the form $\|x - \hat{x}\|_2 \leq Const \cdot \|e\|_2$ from $y = Ax$ provided the RIC$_2$ of $A$ are sufficiently small. The article [20] provides a framework by which RIC$_2$ bounds can be inserted into the recovery conditions, and compressed sensing sampling theorems can be calculated from the resulting equations. Theorem 3.2.3 establishes valid bounds on the RIC$_2$ of Gaussian matrices in the regime considered in Corollary 3.3.1. The claims stated in Corollary 3.3.1 follow directly from substituting the RIC$_2$ bounds of Theorem 3.2.3 into Theorems 2.5.3 – 2.5.5 in Section 2.5.1 originally given as Theorem 10-13 in [20] and solving for the minimum $\gamma$ that satisfies the stated theorems; the calculated values of $\gamma$ have been rounded up to the nearest integer for ease of presentation. Nearly identical values of $\gamma$ can be calculated using the equations from Corollary 3.2.4 rather than the more refined equations in Theorem 3.2.3. □

### 3.5.2 Proof of Corollary 3.3.2

*Proof.* It has been recently shown that Orthogonal Matching Pursuit (OMP) is guaranteed to recover any $k$-sparse vector from its exact measurements provided, [106],

$$\max(L(k,n,N;A), U(k,n,N;A)) < \frac{1}{\sqrt{k-1}}. \tag{3.8}$$

The claimed sampling theorem is obtained by substituting the bound from Theorem 3.2.1 for $\max(L(k,n,N;A), U(k,n,N;A))$ and solving for $n$. □

## 3.6 Proofs of Theorems 3.2.1 - 3.2.3 and Corollary 3.2.4

The proof of Theorems 3.2.1 - 3.2.3 are based upon the previous analysis in [19, 6], differing in the asymptotic limits considered. We need the following definition for the proofs.

**Definition 3.6.1.** *Using Definition 2.2.3, $\psi_{min}(\lambda, \rho)$ and $\psi_{max}(\lambda, \rho)$ are given in (2.2) and*

(2.3) *and* $\lambda^{\min}(\delta,\rho)$ *and* $\lambda^{\max}(\delta,\rho)$ *are the solutions to* (2.4) *and* (2.5)*, respectively, where* $H(\cdot)$ *is the Shannon Entropy function with base e logarithms given in* (1.2)*, we define*

$$\Psi_{\min}(\lambda,\delta,\rho) := \psi_{min}(\lambda^{min}(\delta,\rho),\rho) + \delta^{-1}H(\delta\rho) = 0 \tag{3.9}$$

$$\Psi_{\max}(\lambda,\delta,\rho) := \psi_{max}(\lambda^{max}(\delta,\rho),\rho) + \delta^{-1}H(\delta\rho) = 0 \tag{3.10}$$

Recall that the quantities $\psi_{min}(\lambda,\rho)$ and $\psi_{max}(\lambda,\rho)$ in Definition 2.2.3, and hence Definition 3.6.1, are the large deviation exponents of the lower tail probability density function of the smallest eigenvalue and the upper tail probability density function of the largest eigenvalue of Wishart matrices, respectively. The $\Psi_{\min}(\lambda,\delta,\rho)$ and $\Psi_{\max}(\lambda,\delta,\rho)$ in (3.9) and (3.10), respectively, include a Shannon entropy term from a union bound of the $\binom{N}{k}$ submatrices with $k$ columns. The level curve of $\Psi_{\min}(\lambda,\delta,\rho)$ and $\Psi_{\max}(\lambda,\delta,\rho)$ defines the transition which for $\delta$ and $\rho$ fixed it becomes exponentially unlikely that the smallest eigenvalue is less that $\lambda^{min}(\delta,\rho)$ and the largest eigenvalue is less than $\lambda^{max}(\delta,\rho)$.

The analysis here builds upon the following large deviation bounds on the probability of the sparse eigenvalues exceeding specified values [19, 6]. With $L(k,n,N;A)$ and $U(k,n,N;A)$ defined as in (1.4) and (1.3), respectively, and the definition of $\Psi_{\max}(\lambda(\delta,\rho),\delta,\rho)$ in (3.9) and $\Psi_{\min}(\lambda(\delta,\rho),\delta,\rho)$ in (3.10) these bounds are as follows:

$$Prob\left(\max_{K\subset\Omega,|K|=k}\lambda^{\max}(A_K^*A_K) > \lambda\right) \le poly(n,\lambda)\cdot\exp\left(2n\cdot\Psi_{\max}(\lambda,\delta,\rho)\right), \tag{3.11}$$

and

$$Prob\left(\min_{K\subset\Omega,|K|=k}\lambda^{\min}(A_K^*A_K) > \lambda\right) \le poly(n,\lambda)\cdot\exp\left(2n\cdot\Psi_{\min}(\lambda,\delta,\rho)\right), \tag{3.12}$$

where $poly(z)$ is a (possibly different) polynomial function of its arguments, for explicit formulae see [6]. Theorems 3.2.1 - 3.2.3 follow by proving that for the claimed bounds, the large deviation exponents $n\Psi_{\max}(\lambda(\delta,\rho),\delta,\rho)$ and $n\Psi_{\min}(\lambda(\delta,\rho),\delta,\rho)$ diverge to $-\infty$ as the problem size increases, and do so at a rate sufficiently fast to ensure an overall exponential decay. In addition to establishing the claims of Theorems 3.2.1-3.2.3, we also show that the bounds presented in these theorems cannot be improved upon using the inequalities (3.11) and (3.12), they are in fact sharp leading order asymptotic expansions of the bounds in Theorem 2.2.4.

Throughout the proofs of Theorems 3.2.1-3.2.3 we will be using the following bounds for the Shannon entropy function in (1.2)

$$\begin{aligned}\mathrm{H}(x) &< -x\log x + x, \quad \text{and}\\ \mathrm{H}(x) &> -x\log x + x - x^2;\end{aligned} \tag{3.13}$$

the upper bound follows from (3.14) and the lower bound follows from (3.15),

$$-(1-x)\log(1-x) < x \quad \forall x \in (0,1), \tag{3.14}$$

$$-\log(1-x) > x \quad \forall x < 1 \quad \text{and} \quad x \neq 0. \tag{3.15}$$

### 3.6.1 Theorem 3.2.1

**The Upper Bound,** $\widetilde{\mathcal{U}}^{\rho}(\delta,\rho)$

*Proof.* Define

$$\widetilde{\lambda}^{\max}_{\rho}(\delta,\rho) := 1+\sqrt{2\rho\log\left(\frac{1}{\delta^2\rho^3}\right)+c\rho}, \quad \Rightarrow \quad \widetilde{\mathcal{U}}^{\rho}(\delta,\rho) = \widetilde{\lambda}^{\max}_{\rho}(\delta,\rho)-1$$

as from (3.1). Bounding $\widetilde{\mathcal{U}}^{\rho}(\delta,\rho)$ from above by $(1+\epsilon)\widetilde{\mathcal{U}}^{\rho}(\delta,\rho)$ is equivalent to bounding $\widetilde{\lambda}^{\max}_{\rho}$ from above by $(1+\epsilon)\widetilde{\lambda}^{\max}_{\rho}-\epsilon$. We first establish that for a slightly looser bound, with $c>6$, the exponent $\Psi_{\max}\left((1+\epsilon)\widetilde{\lambda}^{\max}_{\rho}-\epsilon,\delta,\rho\right)$ is negative, and then verify that when multiplied by $n$ it diverges to $-\infty$ as $n$ increases. We also show that for a slightly tighter bound, with $c<6$, $\Psi_{\max}\left((1-\epsilon)\widetilde{\lambda}^{\max}_{\rho}+\epsilon,\delta,\rho\right)$ is positive, and hence the bound $\widetilde{\mathcal{U}}^{\rho}(\delta,\rho)$ cannot be improved using the inequality (3.11) from [19]. We show the above properties, in two parts that for $\delta$ fixed:

1. $\exists\ \rho_0,\ \epsilon>0$ and c $>6$ such that for $\rho<\rho_0, \Psi_{\max}\left((1+\epsilon)\widetilde{\lambda}^{\max}_{\rho}-\epsilon,\delta,\rho\right)\leq 0$;
2. $\nexists\ \rho_0,\ \epsilon>0$ and c $<6$ such that for $\rho<\rho_0, \Psi_{\max}\left((1-\epsilon)\widetilde{\lambda}^{\max}_{\rho}+\epsilon,\delta,\rho\right)\leq 0$,

which are proven below separately as Part 1 and Part 2 respectively.

**Part 1:**

$$\begin{aligned}2\Psi_{\max}\left((1+\epsilon)\widetilde{\lambda}^{\max}_{\rho}-\epsilon,\delta,\rho\right) &= (1+\rho)\log\left((1+\epsilon)\widetilde{\lambda}^{\max}_{\rho}-\epsilon\right)\\ &\quad -\rho\log(\rho)+\rho+1-\left((1+\epsilon)\widetilde{\lambda}^{\max}_{\rho}-\epsilon\right)+\frac{2}{\delta}\mathrm{H}(\delta\rho),\end{aligned} \tag{3.16}$$

by substituting $(1+\epsilon)\widetilde{\lambda}^{\max}_{\rho}-\epsilon$ for $\lambda$ in (3.10). We consolidate notation using $u := \widetilde{\lambda}^{\max}_{\rho}-1$ and using the first bounds of the Shannon entropy in (3.13) we bound (3.16) above as follows

$$\begin{aligned}&2\Psi_{\max}\left((1+\epsilon)\widetilde{\lambda}^{\max}_{\rho}-\epsilon,\delta,\rho\right)\\ &< (1+\rho)\log\left[(1+\epsilon)(1+u)-\epsilon\right]-\rho\log\rho+\rho+1-(1+\epsilon)(1+u)\\ &\quad +\epsilon+\frac{2}{\delta}\left[-\delta\rho\log\left(\delta\rho\right)+\delta\rho\right] \qquad (3.17)\\ &= (1+\rho)\log\left[1+(1+\epsilon)u\right]+\rho\log\left(\frac{1}{\delta^2\rho^3}\right)+\rho-u-\epsilon u+2\delta\rho. \qquad (3.18)\end{aligned}$$

From (3.17) to (3.18) we expand the products of $(1+\epsilon)(1+u)$ and simplify.

Now replacing $\rho \log\left(\frac{1}{\delta^2\rho^3}\right)$ by its equivalent $\frac{1}{2}\left(u^2 - c\rho\right)$ and expanding $(1+\rho)$ in the first term we bound (3.18) by

$$\begin{aligned}
&2\Psi_{\max}\left((1+\epsilon)\widetilde{\lambda}_\rho^{\max} - \epsilon, \delta, \rho\right) \\
&< \log\left(1+u+\epsilon u\right) + \rho\log\left(1+u+\epsilon u\right) + \frac{1}{2}\left(u^2 - c\rho\right) + 3\rho - u - \epsilon u \qquad (3.19)\\
&= \log(1+u) + \log\left(1 + \frac{\epsilon u}{1+u}\right) + \frac{1}{2}u^2 - \frac{1}{2}c\rho + 3\rho - u - \epsilon u \\
&\quad + \rho\log\left(1+u\right) + \rho\log\left(1+\frac{\epsilon u}{1+u}\right) \qquad (3.20)\\
&< u - \frac{1}{2}u^2 + \frac{1}{3}u^3 + \frac{\epsilon u}{1+u} + \frac{1}{2}u^2 - \frac{1}{2}(c-6)\rho - u - \epsilon u + \rho u + \frac{\epsilon\rho u}{1+u}. \qquad (3.21)
\end{aligned}$$

From (3.19) to (3.20) the term $\log(1+u+\epsilon u)$ is factored as in the first two logarithms in (3.20). From (3.20) to (3.21) we bound the first $\log(1+u)$ from above using the second bound in (3.22) and bound above all other logarithmic terms using the first bound in (3.22).

$$\begin{aligned}
\log(1+x) &\leq x, \qquad (3.22)\\
\log(1+x) &\leq x - \frac{1}{2}x^2 + \frac{1}{3}x^3 \quad \forall x > -1.
\end{aligned}$$

We can bound above $\frac{1}{1+u}$ in the fourth and last terms of (3.21) using the bound of (3.23) below.

$$\frac{1}{1+x} < 1 \quad \text{for} \quad 0 < x < 1. \qquad (3.23)$$

Therefore, (3.21) becomes

$$\begin{aligned}
2\Psi_{\max}\left((1+\epsilon)\widetilde{\lambda}_\rho^{\max} - \epsilon, \delta, \rho\right) &< \frac{1}{3}u^3 - \frac{1}{2}(c-6)\rho - \epsilon u + \epsilon u + \rho u + \epsilon\rho u \qquad (3.24)\\
&= -\frac{1}{2}(c-6)\rho + \frac{1}{3}u^3 + (1+\epsilon)\rho u \qquad (3.25)\\
&< -\frac{1}{4}(c-6)\rho - \frac{1}{4}(c-6)\rho + \frac{1}{3}u^3 + \frac{1}{14}(1+\epsilon)u^3 \qquad (3.26)\\
&= -\frac{1}{4}(c-6)\rho - \frac{1}{4}(c-6)\rho + \frac{17+3\epsilon}{42}u^3. \qquad (3.27)
\end{aligned}$$

We simplify (3.24) to get (3.25). From (3.25) to (3.26) we split the first term into half and bound above $\rho u$ by $\frac{1}{14}u^2$ using the fact that by the definition of $u$,

$$u^2 = \rho\left[2\log\left(\frac{1}{\delta^2\rho^3}\right) + 7\right] \quad \Rightarrow \quad \frac{1}{4\log\left(\frac{1}{\delta^2\rho^3}\right)}u^2 < \rho < \frac{1}{14}u^2.$$

Then we simplify from (3.26) to (3.27).

Now in (3.27), if the sum of the last two terms is non-positive there would be a unique $\rho_0$ such that as $\rho \to 0$ for any $\rho < \rho_0$ and fixed $\delta$ (3.27) will be negative. This is achieved if $c > 6$ and

$$-\frac{1}{4}(c-6)\rho + \frac{17+3\epsilon}{42}u^3 \leq 0 \quad \Rightarrow \quad u^3 \leq \frac{21(c-6)}{2(17+3\epsilon)}\rho. \tag{3.28}$$

Since $u$ is strictly decreasing in $\rho$, there is a unique $\rho_0$ that satisfies (3.28) and makes (3.27) negative for $\delta$ fixed, $\epsilon > 0,\ c > 6$ and $\rho < \rho_0$ as $\rho \to 0$.

Having established a negative bound from above and the $\rho_0$ for which it is valid, it remains to show that $n \cdot 2\Psi_{\max}\left((1+\epsilon)\widetilde{\lambda}_\rho^{\max} - \epsilon, \delta, \rho\right) \to -\infty$ as $(k, n, N) \to \infty$. The claimed exponential decay with $k$ follows by noting that $n \cdot \rho = k$, which in conjunction with the first term in the right hand side of (3.27) gives a concluding bound $-\frac{1}{4}(c-6)k$. For $\rho < \rho_0$ therefore

$$Prob\left(U(k,n,N;A) > (1+\epsilon)\widetilde{\mathcal{U}}^\rho(\delta,\rho)\right) \leq poly\left(n, (1+\epsilon)\widetilde{\lambda}_\rho^{\max} - \epsilon\right) \cdot \exp\left[-\frac{(c-6)k}{4}\right].$$

The above bound goes to zero as $k \to \infty$ provided $\frac{\log n}{k} \to 0$ so that the exponential decay in $k$ dominates the polynomial decrease in $n$.

**Part 2:**

$$\begin{aligned}2\Psi_{\max}\left((1-\epsilon)\widetilde{\lambda}_\rho^{\max} + \epsilon, \delta, \rho\right) &= (1+\rho)\log\left((1-\epsilon)\widetilde{\lambda}_\rho^{\max} + \epsilon\right) \\ &\quad - \rho\log(\rho) + \rho + 1 - \left((1-\epsilon)\widetilde{\lambda}_\rho^{\max} + \epsilon\right) + \frac{2}{\delta}\mathrm{H}(\delta\rho), \end{aligned} \tag{3.29}$$

by substituting $(1-\epsilon)\widetilde{\lambda}_\rho^{\max} + \epsilon$ for $\lambda$ in (3.10). We consolidate notation using $u := \widetilde{\lambda}_\rho^{\max} - 1$ and bound the Shannon entropy function from below using the second bound in (3.13) to give

$$\begin{aligned}&2\Psi_{\max}\left((1-\epsilon)\widetilde{\lambda}_\rho^{\max} + \epsilon, \delta, \rho\right) \\ &> (1+\rho)\log\left[(1-\epsilon)(1+u) + \epsilon\right] - \rho\log\rho + \rho + 1 - (1-\epsilon)(1+u) \\ &\quad - \epsilon + \frac{2}{\delta}\left[-\delta\rho\log(\delta\rho) + \delta\rho - \delta^2\rho^2\right] \qquad (3.30) \\ &= (1+\rho)\log\left[1 + (1-\epsilon)u\right] + \rho\log\left(\frac{1}{\delta^2\rho^3}\right) + 3\rho - (1-\epsilon)u - 2\delta\rho^2. \qquad (3.31)\end{aligned}$$

From (3.30) to (3.31) we expand the products of $(1-\epsilon)(1+u)$ and simplify.

Now replacing $\rho\log\left(\frac{1}{\delta^2\rho^3}\right)$ by $\frac{1}{2}\left(u^2 - c\rho\right)$ and expanding $(1+\rho)$ in the first term we have (3.31) become

$$
\begin{aligned}
&2\Psi_{\max}\left((1-\epsilon)\widetilde{\lambda}_\rho^{\max}+\epsilon,\delta,\rho\right)\\
&> \log\left[1+(1-\epsilon)u\right]+\rho\log\left[1+(1-\epsilon)u\right]+\frac{1}{2}\left(u^2-c\rho\right)+3\rho\\
&\quad-(1-\epsilon)u-2\delta\rho^2 &(3.32)\\
&> (1-\epsilon)u-\frac{(1-\epsilon)^2}{2}u^2+\frac{1}{2}u^2-\frac{1}{2}c\rho+3\rho-(1-\epsilon)u+\rho(1-\epsilon)u\\
&\quad-\frac{(1-\epsilon)^2}{2}\rho u^2-2\delta\rho^2 &(3.33)\\
&= \frac{\epsilon(2-\epsilon)}{2}u^2+\frac{1}{2}(6-c)\rho+\rho u-\epsilon\rho u-\frac{(1-\epsilon)}{2}\rho u-2\delta\rho^2 &(3.34)\\
&> \frac{1}{2}(6-c)\rho+\frac{1-\epsilon}{2}\rho u-2\delta\rho^2. &(3.35)
\end{aligned}
$$

From (3.32) to (3.33) we bound below the logarithmic terms by the first two terms of their series expansion using (3.36)

$$\log(1+x)\geq x-\frac{1}{2}x^2 \quad \forall x>-1. \tag{3.36}$$

From (3.33) to (3.34) we bound above $\rho u^2$ and $(1-\epsilon)^2$ by $\rho u$ and $1-\epsilon$, respectively and simplify. Then we dropped the first term to bound below (3.34) by (3.35) and we simplify the terms with $\rho u$.

For $c<6$, the only negative term in (3.35), the last term, goes faster to zero than the rest. Therefore, there does not exist a $\rho_0$, $\epsilon>0$ and $c<6$ such that for $\rho<\rho_0$ and fixed $\delta$ (3.35) is negative. Thus the bound

$$
\begin{aligned}
&Prob\left(U(k,n,N;A)>(1-\epsilon)\widetilde{\mathcal{U}}^\rho(\delta,\rho)\right)\\
&\qquad\leq poly\left(n,(1-\epsilon)\widetilde{\lambda}_\rho^{\max}+\epsilon\right)\cdot\exp\left[2n\Psi_{\max}\left((1-\epsilon)\widetilde{\lambda}_\rho^{\max}+\epsilon,\delta,\rho\right)\right],
\end{aligned}
$$

does not decay to zero as $n\to\infty$.

Now **Part 1** and **Part 2** put together shows that $\widetilde{\mathcal{U}}^\rho(\delta,\rho)$ is a tight upper bound of $U(k,n,N;A)$ with overwhelming probability as the problem size grows in the regime prescribed for $\widetilde{\mathcal{U}}^\rho(\delta,\rho)$ in Theorem 3.2.1. □

### The Lower Bound, $\widetilde{\mathcal{L}}^\rho(\delta,\rho)$

*Proof.* Define

$$\widetilde{\lambda}_\rho^{\min}(\delta,\rho):=1-\sqrt{2\rho\log\left(\frac{1}{\delta^2\rho^3}\right)+c\rho}, \quad \Rightarrow \quad \widetilde{\mathcal{L}}^\rho(\delta,\rho)=1-\widetilde{\lambda}_\rho^{\min}(\delta,\rho)$$

as from (3.1). Since bounding $\widetilde{\mathcal{L}}^{\rho}(\delta,\rho)$ above by $(1+\epsilon)\widetilde{\mathcal{L}}^{\rho}(\delta,\rho)$ is equivalent to bounding $\widetilde{\lambda}_{\rho}^{\min}$ above by $(1+\epsilon)\widetilde{\lambda}_{\rho}^{\min}-\epsilon$. We first establish that for a slightly looser bound, with $c>6$, the exponent $\Psi_{\min}\left((1+\epsilon)\widetilde{\lambda}_{\rho}^{\min}-\epsilon,\delta,\rho\right)$, and then verify that when multiplied by $n$ it diverges to $-\infty$ as $n$ increases. We also show that for a slightly tighter bound, with $c<6$, $\Psi_{\min}\left((1-\epsilon)\widetilde{\lambda}_{\rho}^{\min}+\epsilon,\delta,\rho\right)$ is positive, and hence the bound $\widetilde{\mathcal{L}}^{\rho}(\delta,\rho)$ cannot be improved using the inequality (3.12) from [19]. We show, in two parts that for $\delta$ fixed:

1. $\exists\ \rho_0,\ \epsilon>0$ and c $>6$ such that for $\rho<\rho_0, \Psi_{\min}\left((1+\epsilon)\widetilde{\lambda}_{\rho}^{\min}-\epsilon,\delta,\rho\right)\leq 0$;
2. $\nexists\ \rho_0,\ \epsilon>0$ and c $<6$ such that for $\rho<\rho_0, \Psi_{\min}\left((1-\epsilon)\widetilde{\lambda}_{\rho}^{\min}+\epsilon,\delta,\rho\right)\leq 0$,

which are proven separately in the two parts as follows.

**Part 1:**

$$\begin{aligned}2\Psi_{\min}\left((1+\epsilon)\widetilde{\lambda}_{\rho}^{\min}-\epsilon,\delta,\rho\right) &= 2\mathrm{H}(\rho)+(1-\rho)\log\left((1+\epsilon)\widetilde{\lambda}_{\rho}^{\min}-\epsilon\right)\\ &\quad+\rho\log(\rho)-\rho+1-\left((1+\epsilon)\widetilde{\lambda}_{\rho}^{\min}-\epsilon\right)+\frac{2}{\delta}\mathrm{H}(\delta\rho), \qquad (3.37)\end{aligned}$$

by substituting $(1+\epsilon)\widetilde{\lambda}_{\rho}^{\min}-\epsilon$ for $\lambda$ in (3.9). We consolidate notation using $l:=1-\widetilde{\lambda}_{\rho}^{\min}$ and bound the Shannon entropy functions from above using the first bound in (3.13) which gives

$$\begin{aligned}&2\Psi_{\min}\left((1+\epsilon)\widetilde{\lambda}_{\rho}^{\min}-\epsilon,\delta,\rho\right)\\ &< -2\rho\log(\rho)+2\rho+(1-\rho)\log\left[(1+\epsilon)(1-l)-\epsilon\right]+\rho\log\rho\\ &\quad-\rho+1-(1+\epsilon)(1-l)+\epsilon-2\rho\log(\delta\rho)+\frac{2}{\delta}(\delta\rho) \qquad (3.38)\\ &=(1-\rho)\log(1-l-\epsilon l)+\rho\log\left(\frac{1}{\delta^2\rho^3}\right)+3\rho+l+\epsilon l. \qquad (3.39)\end{aligned}$$

We simplify from (3.38) to (3.39).

Now replacing $\rho\log\left(\frac{1}{\delta^2\rho^3}\right)$ by $\frac{1}{2}\left(l^2-c\rho\right)$ and factoring $(1-l)$ in the argument of the first logarithmic term we have (3.39) become

$$\begin{aligned}&2\Psi_{\min}\left((1+\epsilon)\widetilde{\lambda}_{\rho}^{\min}-\epsilon,\delta,\rho\right)\\ &<(1-\rho)\log(1-l)+(1-\rho)\log\left(1-\frac{\epsilon l}{1-l}\right)+\frac{1}{2}\left(l^2-c\rho\right)+3\rho+l+\epsilon l \qquad (3.40)\\ &<l+\log(1-l)+\frac{1}{2}l^2-\frac{1}{2}c\rho+3\rho-\rho\log(1-l)+\epsilon l-(1-\rho)\frac{\epsilon l}{1-l} \qquad (3.41)\\ &<l-l-\frac{1}{2}l^2+\frac{1}{2}l^2-\frac{1}{2}(c-6)\rho-\rho\log(1-l)+\epsilon l-\epsilon l(1-\rho) \qquad (3.42)\\ &=-\frac{1}{2}(c-6)\rho-\rho\log(1-l)+\epsilon l-\epsilon l+\epsilon\rho l \qquad (3.43)\\ &=-\frac{1}{4}(c-6)\rho-\frac{1}{4}(c-6)\rho-\rho\log(1-l)+\epsilon\rho l. \qquad (3.44)\end{aligned}$$

From (3.40) to (3.41) we expand $(1-\rho)$ and we bound above the second logarithmic term using the first bound of (3.45).

$$\begin{aligned} \log(1-x) &\leq -x, \\ \log(1-x) &\leq -x - \frac{1}{2}x^2, \\ \log(1-x) &\leq -x - \frac{1}{2}x^2 - \frac{1}{3}x^3 \quad \forall x \in (0,1). \end{aligned} \tag{3.45}$$

From (3.41) to (3.42) we bound above the first logarithmic term using the second bound of (3.45) and also bound $\frac{1}{1-l}$ using (3.46).

$$\frac{1}{1-x} \geq 1 \quad \forall x \in (0,1). \tag{3.46}$$

From (3.42) to (3.43) we expand the last brackets and simplify and from (3.43) to (3.44) we simplify and split the first term into two equal terms.

Equation (3.44) is clearly negative if $c > 6$ and the sum of the last three terms is non-positive, which is satisfied if $\epsilon l - \log(1-l) \leq (c-6)/4$, which is also true if, using the first bound in (3.22), $(1+\epsilon)l \leq (c-6)/4$. Since $l$ is strictly increasing in $\rho$, taking on values between zero and 1, there is a unique $\rho_0$ such that for fixed $\delta$, $\epsilon > 0$ and $c > 6$, any $\rho < \rho_0$ satisfies $(1+\epsilon)l \leq (c-6)/4$ and (3.44) is negative.

Having established a negative bound from above and the $\rho_0$ for which it is valid, it remains to show that $n \cdot 2\Psi_{\min}\left((1+\epsilon)\widetilde{\lambda}_\rho^{\min} - \epsilon, \delta, \rho\right) \to -\infty$ as $(k,n,N) \to \infty$, which verifies an exponential decay to zero of the bound (3.12) with $k$. This follows by noting that $n \cdot \rho = k$, which in conjunction with the first term in the right hand side of (3.44) gives a concluding bound $-\frac{1}{4}(c-6)k$. For $\rho < \rho_0$ therefore

$$Prob\left(L(k,n,N;A) > (1+\epsilon)\widetilde{\mathcal{L}}^\rho(\delta,\rho)\right) \leq poly\left(n, (1+\epsilon)\widetilde{\lambda}_\rho^{\min} - \epsilon\right) \cdot \exp\left[-\frac{(c-6)k}{4}\right].$$

The right hand side of which goes to zero as $k \to \infty$ with $\frac{\log n}{k} \to 0$ as $k \to \infty$ so that the exponential decay in $k$ dominates the polynomial decrease in $n$.

**Part 2:**

$$\begin{aligned} 2\Psi_{\min}\left((1-\epsilon)\widetilde{\lambda}_\rho^{\min} + \epsilon, \delta, \rho\right) &= 2\mathrm{H}(\rho) + (1-\rho)\log\left((1-\epsilon)\widetilde{\lambda}_\rho^{\min} + \epsilon\right) \\ &\quad + \rho\log(\rho) - \rho + 1 - \left((1-\epsilon)\widetilde{\lambda}_\rho^{\min} + \epsilon\right) + \frac{2}{\delta}\mathrm{H}(\delta\rho), \end{aligned} \tag{3.47}$$

by substituting $(1-\epsilon)\widetilde{\lambda}_\rho^{\min} + \epsilon$ for $\lambda$ in (3.9). We consolidate notation using $l := 1 - \widetilde{\lambda}_\rho^{\min}$ and bound the Shannon entropy function from below using the second bound in (3.13) to give

$$\begin{aligned}
&2\Psi_{\min}\left((1-\epsilon)\widetilde{\lambda}_{\rho}^{\min}+\epsilon,\delta,\rho\right)\\
&> 2\left[-\rho\log\rho+\rho-\rho^2\right]+(1-\rho)\log\left[(1-\epsilon)(1-l)+\epsilon\right]+\rho\log\rho-\rho\\
&\quad +1-(1-\epsilon)(1-l)-\epsilon+\frac{2}{\delta}\left[-\rho\log(\delta\rho)+\delta\rho-\delta^2\rho^2\right] \qquad (3.48)\\
&= -2\rho\log\rho+2\rho-2\rho^2+(1-\rho)\log\left[1-\epsilon-(1-\epsilon)l+\epsilon\right]+\rho\log\rho-\rho\\
&\quad +1-1+\epsilon+(1-\epsilon)l-\epsilon-2\rho\log(\delta\rho)+2\rho-2\delta\rho^2 \qquad (3.49)\\
&= \log\left[1-(1-\epsilon)l\right]+(1-\epsilon)l-\rho\log\left[1-(1-\epsilon)l\right]+\rho\log\left(\frac{1}{\delta^2\rho^3}\right)\\
&\quad +3\rho-2(1+\delta)\rho^2. \qquad (3.50)
\end{aligned}$$

From (3.48) to (3.49) we expand brackets and simplify and further simplify from (3.49) to (3.50).

Now replacing $\rho\log\left(\frac{1}{\delta^2\rho^3}\right)$ by $\frac{1}{2}\left(l^2-c\rho\right)$, bounding above the second logarithmic term using the first bound of (3.45) and factoring out $\log(1-l)$ we have

$$\begin{aligned}
&2\Psi_{\min}\left((1-\epsilon)\widetilde{\lambda}_{\rho}^{\min}+\epsilon,\delta,\rho\right)\\
&> \log(1-l)+\log\left(1+\frac{\epsilon l}{1-l}\right)+l-\epsilon l+(1-\epsilon)\rho l+\frac{1}{2}\left(l^2-c\rho\right)+3\rho\\
&\quad -2(1+\delta)\rho^2 \qquad (3.51)\\
&> \log(1-l)+l+\frac{1}{2}l^2-\frac{1}{2}c\rho+3\rho-\epsilon l+\log(1+\epsilon l)+\rho l-\epsilon\rho l-2(1+\delta)\rho^2 \qquad (3.52)\\
&> -l-\frac{1}{2}l^2-\frac{1}{2}l^3+l+\frac{1}{2}l^2+\frac{1}{2}(6-c)\rho+\rho l-\epsilon l+\epsilon l-\frac{1}{2}\epsilon^2 l^2-\epsilon\rho l\\
&\quad -2(1+\delta)\rho^2 \qquad (3.53)\\
&= \frac{1}{2}(6-c)\rho-\frac{1}{2}l^3+\rho l-2(1+\delta)\rho^2-\frac{1}{2}\epsilon^2 l^2-\epsilon\rho l. \qquad (3.54)
\end{aligned}$$

From (3.51) to (3.52) we bound below $\frac{1}{1-l}$ using (3.46). From (3.52) to (3.53) we bound below the first logarithmic term using

$$\log(1-x)\geq -x-\frac{1}{2}x^2-\frac{1}{2}x^3 \quad \forall x\in[0,0.44], \qquad (3.55)$$

and also bound below the second logarithmic term using (3.36). From (3.53) to (3.54) we simplify.

The dominant terms in (3.54) are the first two term, all the rest go to zero faster as $\rho\to 0$. Therefore, for (3.54) to be positive as $\rho\to 0$ we need the sum of the first two terms to be positive. This means

$$\frac{1}{2}(6-c)\rho - \frac{1}{2}l^3 > 0 \quad \Rightarrow \quad l^3 < (6-c)\rho. \tag{3.56}$$

This holds for $c < 6$ and small enough $\rho$ and since $l$ is a decreasing function of $\rho^{-1}$ there would not a $\rho_0$ below which this ceases to hold as $\rho \to 0$. Hence we conclude that for fixed $\delta,\ \epsilon > 0$ and $c < 6$ there does not exist a $\rho_0$ such that for $\rho < \rho_0$, (3.54) is negative and $2\Psi_{\min}\left((1-\epsilon)\widetilde{\lambda}_\rho^{\min} + \epsilon, \delta, \rho\right) \leq 0$ as $\rho \to 0$. Thus

$$\begin{aligned} &Prob\left(L(k,n,N;A) > (1-\epsilon)\widetilde{\mathcal{L}}^\rho(\delta,\rho)\right) \\ &\qquad \leq poly\left(n, (1-\epsilon)\widetilde{\lambda}_\rho^{\min} + \epsilon\right) \cdot \exp\left[2n\Psi_{\min}\left((1-\epsilon)\widetilde{\lambda}_\rho^{\min} + \epsilon, \delta, \rho\right)\right], \end{aligned}$$

and as $n \to \infty$ the right hand side of this does not go to zero.

Now **Part 1** and **Part 2** put together shows that $\widetilde{\mathcal{L}}^\rho(\delta,\rho)$ is a tight bound of $L(k,n,N;A)$ with overwhelming probability as the problem size grows in the regime prescribed for $\widetilde{\mathcal{L}}^\rho(\delta,\rho)$ in Theorem 3.2.1. □

### 3.6.2 Theorem 3.2.2

**The Upper Bound, $\widetilde{\mathcal{U}}^\delta(\delta,\rho)$**

*Proof.* Define

$$\widetilde{\lambda}_\delta^{\max}(\delta,\rho) := 1 + 3\rho + \rho\log\left(\frac{1}{\delta^2\rho^3}\right) + (1+\rho)\log\left[c\log\left(\frac{1}{\delta^2\rho^3}\right)\right].$$

It follows from (3.2) that $\widetilde{\mathcal{U}}^\delta(\delta,\rho) = \widetilde{\lambda}_\delta^{\max}(\delta,\rho) - 1$. Bounding $\widetilde{\mathcal{U}}^\delta(\delta,\rho)$ above by $\widetilde{\mathcal{U}}^\delta(\delta,\rho) + \epsilon$ is equivalent to bounding $\widetilde{\lambda}_\delta^{\max}$ above by $\widetilde{\lambda}_\delta^{\max} + \epsilon$. We first establish that for a slightly looser bound, with $c > 1$, the exponent $\Psi_{\max}\left(\widetilde{\lambda}_\delta^{\max} + \epsilon, \delta, \rho\right)$ is negative and then verify that when multiplied by $n$ it diverges to $-\infty$ as $n$ increases. We also show that for a slightly tighter bound, with $c \leq \rho$, the exponent $\Psi_{\max}\left(\widetilde{\lambda}_\delta^{\max} - \epsilon, \delta, \rho\right)$ is bounded from below by zero, and hence the bound $\widetilde{\mathcal{U}}^\delta(\delta,\rho)$ cannot be improved using the inequality (3.11) from [19] We show, in two parts that for $\rho$ fixed:

1. $\exists\ \delta_0,\ \epsilon > 0$ and c $> 1$ such that for $\delta < \delta_0, \Psi_{\max}\left(\widetilde{\lambda}_\delta^{\max} + \epsilon, \delta, \rho\right) \leq 0$;

2. $\nexists\ \delta_0,\ \epsilon > 0$ and c $\leq \rho$ such that for $\delta < \delta_0, \Psi_{\max}\left(\widetilde{\lambda}_\delta^{\max} - \epsilon, \delta, \rho\right) \leq 0$.

which are proven separately in the two parts as follows.

**Part 1:**

$$2\Psi_{\max}\left(\widetilde{\lambda}_{\delta}^{\max}+\epsilon,\delta,\rho\right)=(1+\rho)\log\left(\widetilde{\lambda}_{\delta}^{\max}+\epsilon\right) \\ -\rho\log(\rho)+\rho+1-\left(\widetilde{\lambda}_{\delta}^{\max}+\epsilon\right)+\frac{2}{\delta}\mathrm{H}(\delta\rho), \quad (3.57)$$

by substituting $\widetilde{\lambda}_{\rho}^{\max}+\epsilon$ for $\lambda$ in (3.10). We bound the Shannon entropy function above using the first bound of (3.13) and consolidate notation using $u:=\widetilde{\lambda}_{\rho}^{\max}-1$, then (3.57) becomes

$$\begin{aligned}
&2\Psi_{\max}\left(\widetilde{\lambda}_{\delta}^{\max}+\epsilon,\delta,\rho\right)\\
&<(1+\rho)\log\left[(1+u)+\epsilon\right]-\rho\log\rho+\rho+1-(1+u)-\epsilon+\frac{2}{\delta}\left[-\delta\rho\log\left(\delta\rho\right)+\delta\rho\right] \quad (3.58)\\
&=(1+\rho)\log\left(1+u+\epsilon\right)+\rho\log\left(\frac{1}{\delta^2\rho^3}\right)+3\rho-u-\epsilon. \quad (3.59)
\end{aligned}$$

From (3.58) to (3.59) we simplify. Next where $u$ is not in the logarithmic term we replace it by $\rho\log\left(\frac{1}{\delta^2\rho^3}\right)+(1+\rho)\log\left[c\log\left(\frac{1}{\delta^2\rho^3}\right)\right]+3\rho$ to have

$$\begin{aligned}
&2\Psi_{\max}\left(\widetilde{\lambda}_{\delta}^{\max}+\epsilon,\delta,\rho\right)\\
&<(1+\rho)\log\left(1+u+\epsilon\right)+\rho\log\left(\frac{1}{\delta^2\rho^3}\right)+3\rho-\rho\log\left(\frac{1}{\delta^2\rho^3}\right)-3\rho\\
&\quad-(1+\rho)\log\left[c\log\left(\frac{1}{\delta^2\rho^3}\right)\right]-\epsilon \quad (3.60)\\
&=(1+\rho)\log\left(1+u+\epsilon\right)-\epsilon-(1+\rho)\log\left[c\log\left(\frac{1}{\delta^2\rho^3}\right)\right] \quad (3.61)\\
&=-\alpha(1+\rho)-\epsilon+(1+\rho)\log\left[\frac{1+u+\epsilon}{c\log\left(\frac{1}{\delta^2\rho^3}\right)}\right]+\alpha(1+\rho) \quad (3.62)\\
&=-\alpha-\alpha\rho-\epsilon+(1+\rho)\log\left[\frac{1+u+\epsilon}{c\log\left(\frac{1}{\delta^2\rho^3}\right)}\right]+\alpha(1+\rho)\log e \quad (3.63)\\
&<-\alpha+(1+\rho)\log\left[\frac{e^{\alpha}(1+u+\epsilon)}{c\log\left(\frac{1}{\delta^2\rho^3}\right)}\right]. \quad (3.64)
\end{aligned}$$

From (3.60) to (3.61) we simplify and from (3.61) to (3.62) we combine the logarithmic terms and to create a constant we add $-\alpha(1+\rho)$ and $\alpha(1+\rho)$ for a small positive constant $0<\alpha<1$. From (3.62) to (3.63) we rewrote $\alpha(1+\rho)$ as $\alpha(1+\rho)\log e$. From (3.63) to (3.64) incorporate the second logarithmic term into the first one and we bound above (3.63) by dropping the $-\epsilon$ and $-\alpha\rho$.

Equation (3.64) is clearly negative if the second term is negative, which is satisfied if the argument of the logarithm to be less than one. This leads to

$$e^{-\alpha} c \log\left(\frac{1}{\delta^2\rho^3}\right) \geq u + 1 + \epsilon, \tag{3.65}$$

where again substituting $\rho \log\left(\frac{1}{\delta^2\rho^3}\right) + (1+\rho)\log\log\left(\frac{1}{\delta^2\rho^3}\right) + 3\rho$ for $u$ and reordering the right hand side of (3.65) gives

$$\begin{aligned} e^{-\alpha} c \log\left(\frac{1}{\delta^2\rho^3}\right) \geq \log\log\left(\frac{1}{\delta^2\rho^3}\right) + 1 + \epsilon \\ + \rho\left[3 + \log\left(\frac{1}{\delta^2\rho^3}\right) + \log\log\left(\frac{1}{\delta^2\rho^3}\right)\right]. \end{aligned} \tag{3.66}$$

For small $0 < \alpha < 1$ and $c > 1$, the left hand side of (3.66) is an unbounded strictly increasing function of $\delta^{-1}$ growing exponentially faster than the right hand side of (3.66). Consequently there is a unique $\delta_0$ for which the inequality (3.66) holds for fixed $\rho,\ \epsilon > 0,\ c > 1$ and any $\delta \leq \delta_0$ and as a result making $2\Psi_{\max}\left(\widetilde{\lambda}_\delta^{\max} + \epsilon, \delta, \rho\right) < 0$.

Having established a negative bound from above and the $\delta_0$ for which it is valid, it remains to show that $n \cdot 2\Psi_{\max}\left(\widetilde{\lambda}_\delta^{\max} + \epsilon, \delta, \rho\right) \to -\infty$ as $(k, n, N) \to \infty$, which verifies an exponential decay to zero of the bound (3.11) with $n$. This follows from the first term of the right hand side of (3.64), giving a concluding bound $n(-\alpha)$. For $\delta < \delta_0$ therefore

$$Prob\left(U(k,n,N;A) > \widetilde{\mathcal{U}}^\delta(\delta,\rho) + \epsilon\right) \leq poly\left(n, \widetilde{\lambda}_\delta^{\max} + \epsilon\right) \cdot \exp\left(-\alpha n\right).$$

The right hand side of which goes to zero as $n \to \infty$.

**Part 2:**

$$\begin{aligned} 2\Psi_{\max}\left(\widetilde{\lambda}_\delta^{\max} - \epsilon, \delta, \rho\right) = (1+\rho)\log\left(\widetilde{\lambda}_\delta^{\max} - \epsilon\right) \\ - \rho\log(\rho) + \rho + 1 - \left(\widetilde{\lambda}_\delta^{\max} - \epsilon\right) + \frac{2}{\delta}\mathrm{H}(\delta\rho), \end{aligned} \tag{3.67}$$

by substituting $\widetilde{\lambda}_\rho^{\max} - \epsilon$ for $\lambda$ in (3.10). We lower bound the Shannon entropy function using the second bound of (3.13) and consolidate notation using $u := \widetilde{\lambda}_\delta^{\max} - 1$, then (3.67) becomes

$$\begin{aligned} & 2\Psi_{\max}\left(\widetilde{\lambda}_\delta^{\max} - \epsilon, \delta, \rho\right) \\ & > (1+\rho)\log\left[(1+u) - \epsilon\right] - \rho\log\rho + \rho + 1 - (1+u) + \epsilon \\ & \quad - 2\rho\log(\delta\rho) + \frac{2}{\delta}\left[-\delta\rho\log(\delta\rho) + \delta\rho - \delta^2\rho^2\right] \end{aligned} \tag{3.68}$$

$$= (1+\rho)\log(u + 1 - \epsilon) + \rho\log\left(\frac{1}{\delta^2\rho^3}\right) + 3\rho - u + \epsilon - 2\delta\rho^2 \tag{3.69}$$

$$
\begin{aligned}
&= (1+\rho)\log(u+1-\epsilon) + \rho\log\left(\frac{1}{\delta^2\rho^3}\right) + 3\rho - \rho\log\left(\frac{1}{\delta^2\rho^3}\right) - 3\rho \\
&\quad - (1+\rho)\log\left[c\log\left(\frac{1}{\delta^2\rho^3}\right)\right] + \epsilon - 2\delta\rho^2 && (3.70) \\
&= (1+\rho)\log(u+1-\epsilon) - (1+\rho)\log\left[c\log\left(\frac{1}{\delta^2\rho^3}\right)\right] + \epsilon - 2\delta\rho^2 && (3.71) \\
&= \epsilon + (1+\rho)\log\left[\frac{1+u-\epsilon}{c\log\left(\frac{1}{\delta^2\rho^3}\right)}\right] - 2\delta\rho^2. && (3.72)
\end{aligned}
$$

From (3.68) to (3.69) we simplify. Then from (3.69) to (3.70) we replace $u$ by the expression $\rho\log\left(\frac{1}{\delta^2\rho^3}\right) + (1+\rho)\log\left[c\log\left(\frac{1}{\delta^2\rho^3}\right)\right] + 3\rho$ where $u$ is not in the logarithmic term. From (3.70) to (3.71) we simplify and from (3.71) to (3.72) we combine the logarithmic terms.

The last term in (3.72) obviously goes to zero as $\delta \to 0$, then for the expression to remain positive we need to know how the dominant term, which is the second term, behaves. For this term to be nonnegative as $\delta \to 0$ for fixed $\rho$ we need the argument of the logarithmic to be greater than or equal to 1 which means the following.

$$u + 1 + \epsilon \geq c\log\left(\frac{1}{\delta^2\rho^3}\right).$$

Therefore substituting for $u$ we have

$$\rho\log\left(\frac{1}{\delta^2\rho^3}\right) + (1+\rho)\log\left[c\log\left(\frac{1}{\delta^2\rho^3}\right)\right] + 3\rho + 1 + \epsilon \geq c\log\left(\frac{1}{\delta^2\rho^3}\right),$$

Then we expand the second logarithmic term and rearrange to get

$$(\rho - c)\log\left(\frac{1}{\delta^2\rho^3}\right) + (1+\rho)\log\left[c\log\left(\frac{1}{\delta^2\rho^3}\right)\right] + 3\rho + 1 + \epsilon \geq 0. \tag{3.73}$$

Inequality (3.73) is always true for fixed $\rho$ and $c < \rho$ as $\delta \to 0$. Therefore, we conclude that there does not exists $\delta_0$ such that for any $\rho$ fixed and $\epsilon > 0$ for $\delta < \delta_0$ (3.72) is negative and $2\Psi_{\max}\left(\widetilde{\lambda}_\delta^{\max} - \epsilon, \delta, \rho\right) < 0$ as $\delta \to 0$. Thus

$$\mathit{Prob}\left(U(k,n,N;A) > \widetilde{\mathcal{U}}^\delta(\delta,\rho) - \epsilon\right) \leq \mathit{poly}\left(n, \widetilde{\lambda}_\delta^{\max} - \epsilon\right) \cdot \exp\left[2n\Psi_{\max}\left(\widetilde{\lambda}_\delta^{\max} - \epsilon, \delta, \rho\right)\right],$$

and as $n \to \infty$ the right hand side of this does not necessarily go to zero.

Now **Part 1** and **Part 2** put together shows that $\widetilde{\mathcal{U}}^\delta(\delta,\rho)$ is also a tight upper bound of $U(k,n,N;A)$ with overwhelming probability as the problem size grows in the regime prescribed for $\widetilde{\mathcal{U}}^\delta(\delta,\rho)$ in Theorem 3.2.2. □

**The Lower Bound, $\widetilde{\mathcal{L}}^\delta(\delta,\rho)$**

*Proof.* Define

$$\widetilde{\lambda}_\delta^{\min}(\delta,\rho) := \exp\left(-\frac{3\rho+c}{1-\rho}\right)\cdot\left(\delta^2\rho^3\right)^{\frac{\rho}{1-\rho}}, \quad \Rightarrow \quad \widetilde{\mathcal{L}}^\delta(\delta,\rho) = 1-\widetilde{\lambda}_\delta^{\min}(\delta,\rho)$$

as from (3.3). Bounding $\widetilde{\mathcal{L}}^\delta(\delta,\rho)$ above by $(1+\epsilon)\widetilde{\mathcal{L}}^\delta(\delta,\rho)$ is equivalent to bounding $\widetilde{\lambda}_\delta^{\min}$ above by $(1+\epsilon)\widetilde{\lambda}_\delta^{\min}-\epsilon$. We first establish for a slightly looser bound, with $c>1$, the exponent $\Psi_{\min}\left((1+\epsilon)\widetilde{\lambda}_\delta^{\min}-\epsilon,\delta,\rho\right)$ is negative and then verify that when multiplied by $n$ it diverges to $-\infty$ as $n$ increases. We also show that for a slightly tighter bound, with $c<1$, the exponent $\Psi_{\min}\left((1-\epsilon)\widetilde{\lambda}_\delta^{\min}+\epsilon,\delta,\rho\right)$ is bounded from below by zero, and hence the bound $\widetilde{\mathcal{L}}^\delta(\delta,\rho)$ cannot be improved using the inequality (3.12) from [19]. We show, in two parts that for $\rho$ fixed:

1. $\exists\ \delta_0,\ \epsilon>0$ and c $>1$ such that for $\delta<\delta_0, \Psi_{\min}\left((1+\epsilon)\widetilde{\lambda}_\delta^{\min}-\epsilon,\delta,\rho\right)\le 0$;

2. $\nexists\ \delta_0,\ \epsilon>0$ and c $<1$ such that for $\delta<\delta_0, \Psi_{\min}\left((1-\epsilon)\widetilde{\lambda}_\delta^{\min}+\epsilon,\delta,\rho\right)\le 0$,

which are proven separately in the two parts as follows.

**Part 1:**

$$\begin{aligned}2\Psi_{\min}\left((1+\epsilon)\widetilde{\lambda}_\delta^{\min}-\epsilon,\delta,\rho\right) &= 2\mathrm{H}(\rho)+(1-\rho)\log\left((1+\epsilon)\widetilde{\lambda}_\delta^{\min}-\epsilon\right)\\ &\quad+\rho\log(\rho)-\rho+1-\left((1+\epsilon)\widetilde{\lambda}_\delta^{\min}-\epsilon\right)+\frac{2}{\delta}\mathrm{H}(\delta\rho), \qquad (3.74)\end{aligned}$$

by substituting $(1+\epsilon)\widetilde{\lambda}_\delta^{\min}-\epsilon$ for $\lambda$ in (3.9). We now upper bound the Shannon entropy terms using the first bound of (3.13) and factor out $\widetilde{\lambda}_\delta^{\min}$ for (3.74) to become

$$\begin{aligned}&2\Psi_{\min}\left((1+\epsilon)\widetilde{\lambda}_\delta^{\min}-\epsilon,\delta,\rho\right)\\ &< 2\left[-\rho\log\rho+\rho-\rho^2\right]+(1-\rho)\log\left(\widetilde{\lambda}_\delta^{\min}\right)-(1+\epsilon)\widetilde{\lambda}_\delta^{\min}+\epsilon+1-\rho\\ &\quad+\rho\log\rho+(1-\rho)\log\left[\frac{(1+\epsilon)\widetilde{\lambda}_\delta^{\min}-\epsilon}{\widetilde{\lambda}_\delta^{\min}}\right]+\frac{2}{\delta}\left[-\rho\log\left(\delta\rho\right)+\delta\rho\right] \qquad (3.75)\\ &= (1-\rho)\log\left(\widetilde{\lambda}_\delta^{\min}\right)-(1+\epsilon)\widetilde{\lambda}_\delta^{\min}+\epsilon+(1-\rho)\log\left[(1+\epsilon)-\frac{\epsilon}{\widetilde{\lambda}_\delta^{\min}}\right]\\ &\quad+\rho\log\left(\frac{1}{\delta^2\rho^3}\right)+3\rho+1. \qquad (3.76)\end{aligned}$$

From (3.75) to (3.76) we simplify. Using the fact that by the definition of $\widetilde{\mathcal{L}}^\delta(\delta,\rho)$ in (3.3)

$$\log\left(\widetilde{\lambda}_\delta^{\min}\right) = -\frac{\rho}{1-\rho}\log\left(\frac{1}{\delta^2\rho^3}\right)-\frac{3\rho+c}{1-\rho},$$

we substitute this in (3.76) for $\log\left(\widetilde{\lambda}_\delta^{\min}\right)$ to get

$$\begin{aligned}
&2\Psi_{\min}\left((1+\epsilon)\widetilde{\lambda}_{\delta}^{\min}-\epsilon,\delta,\rho\right)\\
&< (1-\rho)\left[-\frac{\rho}{1-\rho}\log\left(\frac{1}{\delta^2\rho^3}\right)-\frac{3\rho+c}{1-\rho}\right]-(1+\epsilon)\widetilde{\lambda}_{\delta}^{\min}+\epsilon\\
&\quad+(1-\rho)\log\left[(1+\epsilon)-\frac{\epsilon}{\widetilde{\lambda}_{\delta}^{\min}}\right]+\rho\log\left(\frac{1}{\delta^2\rho^3}\right)+3\rho+1 \qquad (3.77)\\
&= -\rho\log\left(\frac{1}{\delta^2\rho^3}\right)-3\rho-c-(1+\epsilon)\widetilde{\lambda}_{\delta}^{\min}+\epsilon+\rho\log\left(\frac{1}{\delta^2\rho^3}\right)\\
&\quad+(1-\rho)\log\left[(1+\epsilon)-\frac{\epsilon}{\widetilde{\lambda}_{\delta}^{\min}}\right]+3\rho+1 \qquad (3.78)\\
&= (1-\rho)\log\left[(1+\epsilon)-\frac{\epsilon}{\widetilde{\lambda}_{\delta}^{\min}}\right]-\widetilde{\lambda}_{\delta}^{\min}-\epsilon\widetilde{\lambda}_{\delta}^{\min}-(c-1)+\epsilon. \qquad (3.79)
\end{aligned}$$

From (3.77) to (3.78) we expand the brackets and from (3.78) to (3.79) we simplify. Now we consolidate notation using $l := 1-\widetilde{\lambda}_{\delta}^{\min}$ and substituting this in (3.79) we have

$$\begin{aligned}
&2\Psi_{\min}\left((1+\epsilon)\widetilde{\lambda}_{\delta}^{\min}-\epsilon,\delta,\rho\right)\\
&< (1-\rho)\log\left[(1+\epsilon)-\frac{\epsilon}{1-l}\right]-(1-l)-\epsilon(1-l)-(c-1)+\epsilon \qquad (3.80)\\
&= -(c-1)+(1-\rho)\log\left(1-\frac{\epsilon l}{1-l}\right)-(1-l)+\epsilon l \qquad (3.81)\\
&< -(c-1)+\epsilon l-(1-\rho)\frac{\epsilon l}{1-l}-(1-l) \qquad (3.82)\\
&= -\frac{1}{2}(c-1)-\frac{1}{2}(c-1)+\epsilon l. \qquad (3.83)
\end{aligned}$$

From (3.80) to (3.81) we simplify and from (3.81) to (3.82) we bound above the logarithmic term using the first bound of (3.45). From (3.82) to (3.83) we drop the third and fourth terms, which are negative, and split the leading term into half. Inequality (3.83) can be further bounded by $-(c-1)/2$ (which will be negative if $c>1$) by choosing $\epsilon$ to be less than $(c-1)/2$ and noting that $l \in (0,1]$.

Having established a negative bound from above and the $\delta_0$ for which it is valid, it remains to show that $n \cdot 2\Psi_{\min}\left((1+\epsilon)\widetilde{\lambda}_{\delta}^{\min}-\epsilon,\delta,\rho\right) \to -\infty$ as $(k,n,N)\to\infty$, which verifies an exponential decay to zero of the bound (3.12) with $n$. This follows from the first term of the right hand side of (3.83) giving a concluding bound $-\frac{1}{2}(c-1)n$. For $\delta<\delta_0$ therefore

$$Prob\left(L(k,n,N;A) > (1+\epsilon)\widetilde{\mathcal{L}}^{\delta}(\delta,\rho)\right) \le poly\left(n,(1+\epsilon)\widetilde{\lambda}_{\delta}^{\min}-\epsilon\right)\cdot\exp\left[-\frac{(c-1)n}{2}\right].$$

The right hand side of which goes to zero as $n\to\infty$.

**Part 2:**

$$
\begin{aligned}
2\Psi_{\min}\left((1-\epsilon)\widetilde{\lambda}_\delta^{\min}+\epsilon,\delta,\rho\right) &= 2\mathrm{H}(\rho)+(1-\rho)\log\left((1-\epsilon)\widetilde{\lambda}_\delta^{\min}+\epsilon\right)\\
&\quad+\rho\log(\rho)-\rho+1-\left((1-\epsilon)\widetilde{\lambda}_\delta^{\min}+\epsilon\right)+\frac{2}{\delta}\mathrm{H}(\delta\rho), \qquad (3.84)
\end{aligned}
$$

by substituting $(1-\epsilon)\widetilde{\lambda}_\delta^{\min}+\epsilon$ for $\lambda$ in (3.9). Next we bound the Shannon entropy functions from below using the second bound in (3.13) to give

$$
\begin{aligned}
&2\Psi_{\min}\left((1-\epsilon)\widetilde{\lambda}_\delta^{\min}+\epsilon,\delta,\rho\right)\\
&> 2\left[-\rho\log\rho+\rho-\rho^2\right]+(1-\rho)\log\left(\widetilde{\lambda}_\delta^{\min}\right)-(1-\epsilon)\widetilde{\lambda}_\delta^{\min}+1-\epsilon+\rho\log\rho\\
&\quad-\rho+(1-\rho)\log\left[\frac{(1-\epsilon)\widetilde{\lambda}_\delta^{\min}+\epsilon}{\widetilde{\lambda}_\delta^{\min}}\right]+\frac{2}{\delta}\left[-\rho\log(\delta\rho)+\delta\rho-\delta^2\rho^2\right] \qquad (3.85)\\
&= (1-\rho)\log\left(\widetilde{\lambda}_\delta^{\min}\right)-(1-\epsilon)\widetilde{\lambda}_\delta^{\min}-\epsilon+(1-\rho)\log\left[(1-\epsilon)+\frac{\epsilon}{\widetilde{\lambda}_\delta^{\min}}\right]\\
&\quad+\rho\log\left(\frac{1}{\delta^2\rho^3}\right)+3\rho+1-2(1+\delta)\rho^2. \qquad (3.86)
\end{aligned}
$$

From (3.85) to (3.86) we simplify. Using the fact that by the definition of $\widetilde{\mathcal{L}}^\delta(\delta,\rho)$ in (3.3)

$$
\log\left(\widetilde{\lambda}_\delta^{\min}\right)=-\frac{\rho}{1-\rho}\log\left(\frac{1}{\delta^2\rho^3}\right)-\frac{3\rho+c}{1-\rho},
$$

we substitute this in (3.86) for $\log\left(\widetilde{\lambda}_\delta^{\min}\right)$ to get

$$
\begin{aligned}
&2\Psi_{\min}\left((1-\epsilon)\widetilde{\lambda}_\delta^{\min}+\epsilon,\delta,\rho\right)\\
&> (1-\rho)\left[-\frac{\rho}{1-\rho}\log\left(\frac{1}{\delta^2\rho^3}\right)-\frac{3\rho+c}{1-\rho}\right]-(1-\epsilon)\widetilde{\lambda}_\delta^{\min}-\epsilon+3\rho\\
&\quad+(1-\rho)\log\left[(1-\epsilon)+\frac{\epsilon}{\widetilde{\lambda}_\delta^{\min}}\right]+\rho\log\left(\frac{1}{\delta^2\rho^3}\right)+1-2(1+\delta)\rho^2 \qquad (3.87)\\
&= -\rho\log\left(\frac{1}{\delta^2\rho^3}\right)-3\rho-c-(1-\epsilon)\widetilde{\lambda}_\delta^{\min}-\epsilon+\rho\log\left(\frac{1}{\delta^2\rho^3}\right)\\
&\quad+(1-\rho)\log\left[(1-\epsilon)+\frac{\epsilon}{\widetilde{\lambda}_\delta^{\min}}\right]+3\rho+1-2(1+\delta)\rho^2 \qquad (3.88)\\
&= (1-\rho)\log\left[(1-\epsilon)+\frac{\epsilon}{\widetilde{\lambda}_\delta^{\min}}\right]-\widetilde{\lambda}_\delta^{\min}+\epsilon\widetilde{\lambda}_\delta^{\min}-\epsilon+1-c-2(1+\delta)\rho^2. \qquad (3.89)
\end{aligned}
$$

From (3.87) to (3.88) we expand the brackets and from (3.88) to (3.89) we simplify. Now we consolidate notation using $l := 1 - \widetilde{\lambda}_\delta^{\min}$ and substituting this in (3.89) we have

$$\begin{aligned}
&2\Psi_{\min}\left((1-\epsilon)\widetilde{\lambda}_\delta^{\min} + \epsilon, \delta, \rho\right) \\
&> (1-\rho)\log\left[(1-\epsilon) + \frac{\epsilon}{1-l}\right] - (1-l) + \epsilon(1-l) - \epsilon + 1 - c - 2(1+\delta)\rho^2 \qquad (3.90) \\
&= (1-\rho)\log\left(1 + \frac{\epsilon l}{1-l}\right) + l - c - \epsilon l - 2(1+\delta)\rho^2 \qquad (3.91) \\
&> (1-\rho)\log(1+\epsilon l) + l - c - \epsilon l - 2(1+\delta)\rho^2 \qquad (3.92) \\
&> (1-\rho)\left(\epsilon l - \frac{1}{2}\epsilon^2 l^2\right) + l - c - \epsilon l - 2(1+\delta)\rho^2 \qquad (3.93) \\
&= \epsilon l - \frac{1}{2}\epsilon^2 l^2 - \epsilon\rho l + \frac{1}{2}\epsilon^2 \rho l^2 + l - c - \epsilon l - 2\rho^2 - 2\delta\rho^2 \qquad (3.94) \\
&= l - c - 2\rho^2 - \epsilon l - \epsilon\rho l - \frac{1}{2}\epsilon^2 l^2 + \frac{1}{2}\epsilon^2\rho l^2 - 2\delta\rho^2. \qquad (3.95)
\end{aligned}$$

We simplify from (3.90) to (3.91) and from (3.91) to (3.92) we bound below $\frac{1}{1-l}$ using the bound of (3.46). From (3.92) to (3.93) we bound below the logarithmic term using the bound of (3.36). From (3.93) to (3.94) we expand the brackets and from (3.94) to (3.95) we simplify.

The leading terms of (3.95) are the first three and $l$ is strictly increasing as $\delta^{-1}$ approaches 1. If $c < 1$, there will be some values of $\rho$ for which (3.95) will always be positive as $\delta \to 0$. Thus there does not exist any $\delta_0$ such that for any $\rho$ fixed, $\epsilon > 0,\ c < 1$ and $\delta < \delta_0$, (3.95) becomes negative. Thus

$$\begin{aligned}
&Prob\left(L(k,n,N;A) > (1-\epsilon)\widetilde{\mathcal{L}}^\delta(\delta,\rho)\right) \\
&\qquad \le poly\left(n, (1-\epsilon)\widetilde{\lambda}_\delta^{\min} + \epsilon\right) \cdot \exp\left[2n\Psi_{\min}\left((1-\epsilon)\widetilde{\lambda}_\delta^{\min} + \epsilon, \delta, \rho\right)\right],
\end{aligned}$$

and as $n \to \infty$ the right hand side of this does not necessarily go to zero.

Now **Part 1** and **Part 2** put together shows that $\widetilde{\mathcal{L}}^\delta(\delta,\rho)$ is also a tight bound of $L(k,n,N;A)$ with overwhelming probability as the sample size grows in the regime prescribed for $\widetilde{\mathcal{L}}^\delta(\delta,\rho)$ in Theorem 3.2.2. □

### 3.6.3 Theorem 3.2.3

**The Upper Bound, $\widetilde{\mathcal{U}}^\gamma(\delta, \rho_\gamma(\delta))$**

*Proof.* To simplify notation we will use $\rho$ for $\rho_\gamma(\delta)$ in the proof. Lets define

$$\widetilde{\lambda}_\gamma^{\max}(\delta,\rho) := 1 + \sqrt{2\rho\log\left(\frac{1}{\delta^2\rho^3}\right) + 6\rho} + c_u\left[2\rho\log\left(\frac{1}{\delta^2\rho^3}\right) + 6\rho\right].$$

It follows from (3.4) that $\widetilde{\mathcal{U}}^{\gamma}(\delta,\rho) = \widetilde{\lambda}_{\gamma}^{\max}(\delta,\rho) - 1$. Bounding $\widetilde{\mathcal{U}}^{\gamma}(\delta,\rho)$ above by $\widetilde{\mathcal{U}}^{\gamma}(\delta,\rho)+\epsilon$ is equivalent to bounding $\widetilde{\lambda}_{\gamma}^{\max}$ above by $\widetilde{\lambda}_{\gamma}^{\max}+\epsilon$. We first establish that for a slightly looser bound, with $c_u > 1/3$, the exponent $\Psi_{\max}\left(\widetilde{\lambda}_{\gamma}^{\max}+\epsilon,\delta,\rho\right)$ is negative and then verify that when multiplied by $n$ it diverges to $-\infty$ as $n$ increases. We also show that for a slightly tighter bound, with $c_u \le 1/5$, the exponent $\Psi_{\max}\left(\widetilde{\lambda}_{\gamma}^{\max}-\epsilon,\delta,\rho\right)$ is bounded from below by zero, and hence the bound $\widetilde{\mathcal{U}}^{\gamma}(\delta,\rho)$ cannot be improved using the inequality (3.11) from [19]. We show, in two parts that for $\gamma > \gamma_0$ fixed:

1. $\exists\ \delta_0,\ \epsilon > 0$ and $\mathrm{c_u} > 1/3$ such that for $\delta < \delta_0, \Psi_{\max}\left(\widetilde{\lambda}_{\gamma}^{\max}+\epsilon,\delta,\rho\right) \le 0$;

2. $\nexists\ \delta_0,\ \epsilon > 0$ and $\mathrm{c_u} \le 1/5$ such that for $\delta < \delta_0, \Psi_{\max}\left(\widetilde{\lambda}_{\gamma}^{\max}-\epsilon,\delta,\rho\right) \le 0$.

which are proven separately in the two parts.

**Part 1:**

$$2\Psi_{\max}\left(\widetilde{\lambda}_{\gamma}^{\max}+\epsilon,\delta,\rho\right) = (1+\rho)\log\left(\widetilde{\lambda}_{\gamma}^{\max}+\epsilon\right) - \rho\log(\rho) + \rho + 1 - \widetilde{\lambda}_{\gamma}^{\max} - \epsilon + \frac{2}{\delta}H(\delta\rho), \quad (3.96)$$

by substituting $\widetilde{\lambda}_{\gamma}^{\max}+\epsilon$ for $\lambda$ in the definition of $\Psi_{\max}(\lambda,\delta,\rho)$ in (3.10).

Now letting $u = \widetilde{\lambda}_{\gamma}^{\max}-1$ and substituting this in (3.96) and upper bounding the Shannon entropy term using the first bound of (3.13) gives (3.97) below

$$\begin{aligned}
&2\Psi_{\max}\left(\widetilde{\lambda}_{\gamma}^{\max}+\epsilon,\delta,\rho\right)\\
&< (1+\rho)\log(1+u+\epsilon) - \rho\log(\rho) + \rho + 1 - (1+u) - \epsilon\\
&\quad + \frac{2}{\delta}\left[-\delta\rho\log(\delta\rho) + \delta\rho\right] && (3.97)\\
&= \log(1+u+\epsilon) + \rho\log(1+u+\epsilon) - u - \epsilon + \rho\log\left(\frac{1}{\delta^2\rho^3}\right) + 3\rho && (3.98)\\
&= \log(1+u) + \log\left(1+\frac{\epsilon}{1+u}\right) + \rho\log(1+u+\epsilon) - u - \epsilon\\
&\quad + \rho\log\left(\frac{1}{\delta^2\rho^3}\right) + 3\rho && (3.99)\\
&< -u + u - \frac{1}{2}u^2 + \frac{1}{3}u^3 + \rho\log\left(\frac{1}{\delta^2\rho^3}\right) + 3\rho + \rho\log(1+u+\epsilon) - \epsilon\\
&\quad + \log(1+\epsilon) && (3.100)\\
&< -\frac{1}{2}u^2 + \frac{1}{3}u^3 + \rho\log\left(\frac{1}{\delta^2\rho^3}\right) + 3\rho + \rho\log(1+u+\epsilon) - \epsilon + \epsilon. && (3.101)
\end{aligned}$$

From (3.97) to (3.98) we expand the $(1+\rho)$ in the first term and simplify while from (3.98) to (3.99) we expand the first logarithmic term. From (3.99) to (3.100) we bound above $\log(1+u)$ and $\frac{1}{1+u}$ using the second bound of (3.22) and the bound of (3.23) respectively. Then from (3.100) to (3.101) we simplify and bound above $\log(1+\epsilon)$ using the first bound of (3.22).

Let $x = 2\rho \log\left(\frac{1}{\delta^2\rho^3}\right) + 6\rho$ which means $u = \sqrt{x} + c_u x$. We simplify (3.101) and replace the sum of the second two terms by $\frac{1}{2}x$ and $u$ in the first two terms by $\sqrt{x} + c_u x$ to get

$$\begin{aligned}
&2\Psi_{\max}\left(\widetilde{\lambda}_{\gamma}^{\max} + \epsilon, \delta, \rho\right) \\
&< -\frac{1}{2}\left(\sqrt{x} + c_u x\right)^2 + \frac{1}{3}\left(\sqrt{x} + c_u x\right)^3 + \frac{1}{2}x + \rho\log(1+u+\epsilon) \qquad (3.102) \\
&= -\frac{1}{2}x - c_u x^{3/2} - \frac{1}{2}c_u^2 x^2 + \frac{1}{3}x^{3/2} + c_u x^2 + c_u^2 x^{5/2} + \frac{1}{3}c_u^3 x^3 + \frac{1}{2}x \\
&\quad + \rho\log(1+u+\epsilon) \qquad (3.103) \\
&= -\left(c_u - \frac{1}{3}\right)x^{3/2} + c_u x^2 - \frac{1}{2}c_u^2 x^2 + c_u^2 x^{5/2} + \frac{1}{3}c_u^3 x^3 + \rho\log(1+u+\epsilon). \qquad (3.104)
\end{aligned}$$

From (3.102) to (3.103) we expand the first two brackets and from (3.103) to (3.104) we simplify. Substituting $1/\left[\gamma\log\left(\frac{1}{\delta}\right)\right]$ for $\rho$ in the expression for $x$ we have $x = 4/\gamma + g(\rho)$ where $g(\rho) = 6\rho\log(1/\rho) + 6\rho$ and goes to zero with $\delta$. Therefore, if $4/\gamma < 1$ for $\delta$ small enough we will have $x < 1$. This means for $\gamma > 4$ we can define $\delta_1$ such that for $\delta < \delta_1$, $x < 1$ and we can upper bound $x^{5/2}$ and $x^3$ by $x^2$ since $x^2 > x^{2+j}$ for $j > 0$ when $x < 1$. Using this fact we can bound (3.104) above to get

$$\begin{aligned}
&2\Psi_{\max}\left(\widetilde{\lambda}_{\gamma}^{\max} + \epsilon, \delta, \rho\right) \\
&< -\left(c_u - \frac{1}{3}\right)x^{3/2} + c_u x^2 - \frac{1}{2}c_u^2 x^2 + c_u^2 x^2 + \frac{1}{3}c_u^3 x^2 + \rho\log(1+u+\epsilon) \qquad (3.105) \\
&= -\frac{1}{2}\left(c_u - \frac{1}{3}\right)x^{3/2} - \frac{1}{2}\left(c_u - \frac{1}{3}\right)x^{3/2} + c_u x^2 + \frac{1}{2}c_u^2 x^2 + \frac{1}{3}c_u^3 x^2 \\
&\quad + \rho\log(1+u+\epsilon). \qquad (3.106)
\end{aligned}$$

From (3.105) to (3.106) we simplify and split the first term into half. The last term goes to zero with $\delta$ so we can define $\delta_2$ such that for $\delta < \delta_2$ we can bound this term above by $x^2$. But also $x^{3/2} = 8/\sqrt{\gamma^3} + G(\rho)$ where $G(\rho)$ is the difference between $[4/\gamma + g(\rho)]^{3/2}$ and $(4/\gamma)^{3/2}$ which also goes to zero with $\delta$ because this difference is a sum of products with $g(\rho)$. This means $-x^{3/2} < -8/\sqrt{\gamma^3}$ since $g(\rho)$ is positive. Now let $f_u(c_u) = c_u + \frac{1}{2}c_u^2 + \frac{1}{3}c_u^3$, which is positive for all $c_u > 0$, using the above therefore we can bound (3.106) to get

$$\begin{aligned}
&2\Psi_{\max}\left(\widetilde{\lambda}_{\gamma}^{\max} + \epsilon, \delta, \rho\right) \\
&< \frac{1}{2}\left(c_u - \frac{1}{3}\right)\cdot\left(-\frac{8}{\sqrt{\gamma^3}}\right) - \frac{1}{2}\left(c_u - \frac{1}{3}\right)x^{3/2} + f_u(c_u)x^2 + x^2 \qquad (3.107) \\
&= -\frac{4}{\sqrt{\gamma^3}}\left(c_u - \frac{1}{3}\right) - \frac{1}{2}\left(c_u - \frac{1}{3}\right)x^{3/2} + \left[1 + f_u(c_u)\right]x^2. \qquad (3.108)
\end{aligned}$$

From (3.107) to (3.108) we simplify. For (3.108) to be negative all we need is for $c_u > 1/3$ and the sum of the last two terms to be non positive, that is:

$$-\frac{1}{2}\left(c_u - \frac{1}{3}\right)x^{3/2} + \left[1 + f_u(c_u)\right]x^2 \leq 0 \quad \Rightarrow \quad x \leq \left\{\frac{3c_u - 1}{6\left[1 + f_u(c_u)\right]}\right\}^2. \tag{3.109}$$

Let's define $\delta_3$ such that for $\delta < \delta_3$ (3.109) holds; since $x$ is a decreasing function of $\delta^{-1}$ for fixed $\gamma$ there exist a unique $\delta_3$. We set $\delta_0 = \min(\delta_1, \delta_2, \delta_3)$ and conclude that if $c_u > 1/3$, for fixed $\gamma > \gamma_0 = 4$ and $\epsilon > 0$ when $\delta < \delta_0$ as $\delta \to 0$ (3.108) will remain negative and $2\Psi_{\max}\left(\widetilde{\lambda}_\gamma^{\max} + \epsilon, \delta, \rho\right) < 0$.

Having established a negative bound from above and the $\delta_0$ for which it is valid, it remains to show that $n \cdot 2\Psi_{\max}\left(\widetilde{\lambda}_\gamma^{\max} + \epsilon, \delta, \rho\right) \to -\infty$ as $(k, n, N) \to \infty$, which verifies an exponential decay to zero of the bound (3.11) with $n$. This follows from the first term of the right hand side of (3.108), giving a concluding bound $-n \cdot \frac{4}{\sqrt{\gamma^3}}\left(c_u - \frac{1}{3}\right)$. For fixed $\gamma > \gamma_0$ and $\delta < \delta_0$ therefore

$$Prob\left(U(k,n,N;A) > \widetilde{\mathfrak{U}}^\gamma(\delta,\rho) + \epsilon\right) \leq poly\left(n, \widetilde{\lambda}_\gamma^{\max} + \epsilon\right) \cdot \exp\left[-\frac{4n}{\sqrt{\gamma^3}}\left(c_u - \frac{1}{3}\right)\right].$$

The right hand side of which goes to zero as $n \to \infty$.

**Part 2:**

$$\begin{aligned}2\Psi_{\max}\left(\widetilde{\lambda}_\gamma^{\max} - \epsilon, \delta, \rho\right) &= (1+\rho)\log\left(\widetilde{\lambda}_\gamma^{\max} - \epsilon\right) - \rho\log(\rho) \\ &\quad + \rho + 1 - \widetilde{\lambda}_\gamma^{\max} + \epsilon + \frac{2}{\delta}H(\delta\rho),\end{aligned} \tag{3.110}$$

by substituting $\widetilde{\lambda}_\gamma^{\max} - \epsilon$ for $\lambda$ in the definition of $\Psi_{\max}(\lambda, \delta, \rho)$ in (3.10).

Now letting $u = \widetilde{\lambda}_\gamma^{\max} - 1$ and substituting this in (3.110) and lower bounding the Shannon entropy term using the second bound of (3.13) gives (3.111) below

$$\begin{aligned}&2\Psi_{\max}\left(\widetilde{\lambda}_\gamma^{\max} - \epsilon, \delta, \rho\right) \\ &> (1+\rho)\log(1+u-\epsilon) - \rho\log(\rho) + \rho + 1 - (1+u) + \epsilon \\ &\quad + \frac{2}{\delta}\left[-\delta\rho\log(\delta\rho) + \delta\rho - \delta^2\rho^2\right] && (3.111) \\ &= \log(1+u-\epsilon) + \rho\log(1+u-\epsilon) - u + \epsilon + \rho\log\left(\frac{1}{\delta^2\rho^3}\right) + 3\rho - 2\delta\rho^2 && (3.112) \\ &= \log(1+u) + \log\left(1 - \frac{\epsilon}{1+u}\right) + \rho\log(1+u-\epsilon) - u + \epsilon \\ &\quad + \rho\log\left(\frac{1}{\delta^2\rho^3}\right) + 3\rho - 2\delta\rho^2 && (3.113)\end{aligned}$$

$$
\begin{aligned}
&> -u + u - \frac{1}{2}u^2 + \frac{1}{5}u^3 + \rho \log\left(\frac{1}{\delta^2\rho^3}\right) + 3\rho + \epsilon + \log(1-\epsilon) \\
&\quad + \rho\log(1+u-\epsilon) - 2\delta\rho^2 \qquad (3.114) \\
&= -\frac{1}{2}u^2 + \frac{1}{5}u^3 + \rho \log\left(\frac{1}{\delta^2\rho^3}\right) + 3\rho + \epsilon + \log(1-\epsilon) + \rho\log(1+u-\epsilon) - 2\delta\rho^2. \qquad (3.115)
\end{aligned}
$$

From (3.111) to (3.112) we expand the $(1+\rho)$ in the first term and simplify while from (3.112) to (3.113) we expand the first logarithmic term. From (3.113) to (3.114) we bound above $\frac{1}{1+u}$ using the bound of (3.23) and bound below $\log(1+u)$ using the following bound.

$$
\log(1+x) \geq x - \frac{1}{2}x^2 + \frac{1}{5}x^3 \quad \forall x \in [0, 0.92]. \qquad (3.116)
$$

From (3.114) to (3.115) we simplify.

Let $x = 2\rho\log\left(\frac{1}{\delta^2\rho^3}\right) + 6\rho$ which means $u = \sqrt{x} + c_u x$. We simplify (3.115) and replace the second two terms by $\frac{1}{2}x$ and $u$ in the first two terms by $\sqrt{x} + c_u x$ to get

$$
\begin{aligned}
&2\Psi_{\max}\left(\widetilde{\lambda}_\gamma^{\max} - \epsilon, \delta, \rho\right) \\
&> -\frac{1}{2}\left(\sqrt{x} + c_u x\right)^2 + \frac{1}{5}\left(\sqrt{x} + c_u x\right)^3 + \frac{1}{2}x + \epsilon + \log(1-\epsilon) \\
&\quad + \rho\log(1+u-\epsilon) - 2\delta\rho^2 \qquad (3.117) \\
&= -\frac{1}{2}x - c_u x^{3/2} - \frac{1}{2}c_u^2 x^2 + \frac{1}{5}x^{3/2} + \frac{3}{5}c_u x^2 + \frac{3}{5}c_u^2 x^{5/2} + \frac{1}{5}c_u^3 x^3 + \frac{1}{2}x \\
&\quad + \epsilon + \log(1-\epsilon) + \rho\log(1+u-\epsilon) - 2\delta\rho^2 \qquad (3.118) \\
&= \left(\frac{1}{5} - c_u\right)x^{3/2} + c_u\left(1 - \frac{1}{2}c_u\right)x^2 + \frac{3}{5}c_u^2 x^{5/2} + \frac{1}{5}c_u^3 x^3 + \rho\log(1+u-\epsilon) \\
&\quad + \epsilon + \log(1-\epsilon) - 2\delta\rho^2. \qquad (3.119)
\end{aligned}
$$

From (3.117) to (3.118) we expand the first two brackets and from (3.118) to (3.119) we simplify. The dominant terms that does not go to zero as $\delta \to 0$ are the terms with $x$ and their sum is positive for $c_u \leq 1/5$. Hence for fixed $\gamma$ there does not exist a $\delta_0$ such that $2\Psi_{\max}\left(\widetilde{\lambda}_\gamma^{\max} - \epsilon, \delta, \rho\right) \leq 0$. Thus

$$
\mathit{Prob}\left(U(k,n,N;A) > \widetilde{\mathcal{U}}^\gamma(\delta,\rho) - \epsilon\right) \leq \mathit{poly}\left(n, \widetilde{\lambda}_\gamma^{\max} - \epsilon\right) \cdot \exp\left[2n\Psi_{\max}\left(\widetilde{\lambda}_\gamma^{\max} - \epsilon, \delta, \rho\right)\right],
$$

and as $n \to \infty$ the right hand side of this does not go to zero.

Now **Part 1** and **Part 2** put together shows that $\widetilde{\mathcal{U}}^\gamma(\delta,\rho)$ is also a tight upper bound of $U(k,n,N;A)$ with overwhelming probability as the problem size grows in the regime prescribed for $\widetilde{\mathcal{U}}^\gamma(\delta,\rho)$ in Theorem 3.2.3. □

**The Lower Bound, $\widetilde{\mathcal{L}}^{\gamma}(\delta, \rho_{\gamma}(\delta))$**

*Proof.* Lets also define

$$\widetilde{\lambda}_{\gamma}^{\min}(\delta, \rho) := 1 - \sqrt{2\rho \log\left(\frac{1}{\delta^2\rho^3}\right) + 6\rho} + c_l \left[2\rho\log\left(\frac{1}{\delta^2\rho^3}\right) + 6\rho\right].$$

This implies that $\widetilde{\mathcal{L}}^{\gamma}(\delta,\rho) = 1 - \widetilde{\lambda}_{\gamma}^{\min}(\delta,\rho)$ following from (3.5). Bounding $\widetilde{\mathcal{L}}^{\gamma}(\delta,\rho)$ above by $\widetilde{\mathcal{L}}^{\gamma}(\delta,\rho) + \epsilon$ is equivalent to bounding $\widetilde{\lambda}_{\gamma}^{\min}$ below by $\widetilde{\lambda}_{\gamma}^{\min} - \epsilon$. We first establish that for a slightly looser bound, with $c_l > 1/3$, the exponent $\Psi_{\min}\left(\widetilde{\lambda}_{\gamma}^{\min} - \epsilon, \delta, \rho\right)$ is negative and then verify that when multiplied by $n$ it diverges to $-\infty$ as $n$ increases. We also show that for a slightly tighter bound, with $c_l < 1/3$, the exponent $\Psi_{\min}\left(\widetilde{\lambda}_{\gamma}^{\min} + \epsilon, \delta, \rho\right)$ is bounded from below by zero, and hence the bound $\widetilde{\mathcal{L}}^{\gamma}(\delta,\rho)$ cannot be improved using the inequality (3.12) from [19]. We show, in two parts that for $\gamma > \gamma_0$ fixed:

1. $\exists\ \delta_0,\ \epsilon > 0$ and $\mathrm{c_l} < 1/3$ such that for $\delta < \delta_0, \Psi_{\min}\left(\widetilde{\lambda}_{\gamma}^{\min} - \epsilon, \delta, \rho\right) \leq 0$;
2. $\nexists\ \delta_0,\ \epsilon > 0$ and $\mathrm{c_l} \geq 1/2$ such that for $\delta < \delta_0, \Psi_{\min}\left(\widetilde{\lambda}_{\gamma}^{\min} + \epsilon, \delta, \rho\right) \leq 0$,

which are proven separately in the two parts as follows.

**Part 1:**

$$\begin{aligned} 2\Psi_{\min}\left(\widetilde{\lambda}_{\gamma}^{\min} - \epsilon, \delta, \rho\right) &= 2\mathrm{H}(\rho) + (1-\rho)\log\left(\widetilde{\lambda}_{\gamma}^{\min} - \epsilon\right) \\ &\quad + \rho\log(\rho) - \rho + 1 - \left(\widetilde{\lambda}_{\gamma}^{\min} - \epsilon\right) + \frac{2}{\delta}\mathrm{H}(\delta\rho), \end{aligned} \tag{3.120}$$

by substituting $\widetilde{\lambda}_{\gamma}^{\min} - \epsilon$ for $\lambda$ in (3.9). Let $l := 1 - \widetilde{\lambda}_{\gamma}^{\min}$ and bound the Shannon entropy functions from above using the first bound in (3.13) which gives

$$\begin{aligned} &2\Psi_{\min}\left(\widetilde{\lambda}_{\gamma}^{\min} - \epsilon, \delta, \rho\right) \\ &< -2\rho\log(\rho) + 2\rho + (1-\rho)\log\left[(1-l) - \epsilon\right] + \rho\log\rho - \rho + 1 - (1-l) \\ &\quad + \epsilon - 2\rho\log(\delta\rho) + \frac{2}{\delta}(\delta\rho) && (3.121) \\ &= (1-\rho)\log(1-l-\epsilon) + \rho\log\left(\frac{1}{\delta^2\rho^3}\right) + 3\rho + l + \epsilon && (3.122) \\ &= l + \log(1-l) + \epsilon + \log\left(1 - \frac{\epsilon}{1-l}\right) - \rho\log(1-l-\epsilon) + \rho\log\left(\frac{1}{\delta^2\rho^3}\right) + 3\rho && (3.123) \\ &< l + -l - \frac{1}{2}l^2 - \frac{1}{3}l^3 + \rho\log\left(\frac{1}{\delta^2\rho^3}\right) + 3\rho - \rho\log(1-l-\epsilon) + \log(1-\epsilon) + \epsilon && (3.124) \\ &< -\frac{1}{2}l^2 - \frac{1}{3}l^3 + \rho\log\left(\frac{1}{\delta^2\rho^3}\right) + 3\rho - \rho\log(1-l-\epsilon) - \epsilon + \epsilon. && (3.125) \end{aligned}$$

We simplify from (3.121) to (3.122) and from (3.122) to (3.123) we expand the first logarithmic term. From (3.123) to (3.124) we bound $\frac{1}{1-l}$ below and $\log(1-l)$ above using

(3.46) and the third bound of (3.45) respectively. From (3.124) to (3.125) we simplify and bound above $\log(1-\epsilon)$ using the first bound of (3.45).

Let $x = 2\rho \log\left(\frac{1}{\delta^2\rho^3}\right) + 6\rho$ which means $l = \sqrt{x} - c_l x$. We simplify (3.125) and replace the second two terms by $\frac{1}{2}x$ and $l$ in the first two terms by $\sqrt{x} - c_l x$ to get

$$\begin{aligned}
&2\Psi_{\min}\left(\widetilde{\lambda}_\gamma^{\min} - \epsilon, \delta, \rho\right) \\
&< -\frac{1}{2}\left(\sqrt{x} - c_l x\right)^2 - \frac{1}{3}\left(\sqrt{x} - c_l x\right)^3 + \frac{1}{2}x - \rho \log\left(1 - l - \epsilon\right) && (3.126)\\
&= -\frac{1}{2}x + c_l x^{3/2} - \frac{1}{2}c_l^2 x^2 - \frac{1}{3}x^{3/2} + c_l x^2 - c_l^2 x^{5/2} + \frac{1}{3}c_l^3 x^3 + \frac{1}{2}x \\
&\quad - \rho \log\left(1 - l - \epsilon\right) && (3.127)\\
&= -\left(\frac{1}{3} - c_l\right) x^{3/2} + c_l x^2 - \frac{1}{2}c_l^2 x^2 - c_l^2 x^{5/2} + \frac{1}{3}c_l^3 x^3 - \rho \log\left(1 - l - \epsilon\right). && (3.128)
\end{aligned}$$

From (3.126) to (3.127) we expand the first two brackets and from (3.127) to (3.128) we simplify.

Substituting $1/\left[\gamma \log\left(1/\delta\right)\right]$ for $\rho$ in the expression for $x$ we have $x = 4/\gamma + g(\rho)$ where $g(\rho) = 6\rho \log\left(1/\rho\right) + 6\rho$ and goes to zero with $\delta$. We make the same argument as in **Part 1** of the proof for $\widetilde{\mathfrak{U}}^\gamma(\delta, \rho_\gamma(\delta))$ in Section 3.6.3, that is for $\gamma > 4$ we can define $\delta_1$ such that for $\delta < \delta_1,\ x < 1$ and we can upper bound $x^3$ by $x^2$ since $x^2 > x^{2+j}$ for $j > 0$ when $x < 1$. The last term in (3.128) goes to zero with $\delta$, so we can define $\delta_2$ such that for $\delta < \delta_2$ we can bound this term above by $x^2$ which is a constant. We split the first term of (3.128) into half and drop the two $c_l^2$ terms because they are negative. Let $f_l(c_l) = c_l + \frac{1}{3}c_l^3$, which is positive for all $c_l > 0$, using the above we upper bound (3.128) as follows.

$$\begin{aligned}
2\Psi_{\min}\left(\widetilde{\lambda}_\gamma^{\min} - \epsilon, \delta, \rho\right) &< -\frac{1}{2}\left(\frac{1}{3} - c_l\right) x^{3/2} - \frac{1}{2}\left(\frac{1}{3} - c_l\right) x^{3/2} + f_l(c_l)x^2 + x^2 && (3.129)\\
&< -\frac{4}{\sqrt{\gamma^3}}\left(\frac{1}{3} - c_l\right) - \frac{1}{2}\left(\frac{1}{3} - c_l\right) x^{3/2} + \left[1 + f_l(c_l)\right] x^2. && (3.130)
\end{aligned}$$

From (3.129) to (3.130) we use the fact that $-x^{3/2} < -8/\sqrt{\gamma^3}$ as shown in Section 3.6.3. For (3.130) to be negative all we need is for $c_l < 1/3$ and the sum of the last two terms to be non positive, that is:

$$-\frac{1}{2}\left(\frac{1}{3} - c_l\right) x^{3/2} + \left[1 + f_l(c_l)\right] x^2 \leq 0 \quad \Rightarrow \quad x \leq \left\{\frac{1 - 3c_l}{6\left[1 + f_l(c_l)\right]}\right\}^2. \qquad (3.131)$$

Let's define $\delta_3$ such that for $\delta < \delta_3$ (3.131) holds; since $x$ is a decreasing function of $\delta^{-1}$ for fixed $\gamma$ there exist a unique $\delta_3$. We set $\delta_0 = \min\left(\delta_1, \delta_2, \delta_3\right)$ and conclude that if $c_l < 1/3$, for fixed $\gamma > \gamma_0 = 4$ and $\epsilon > 0$ when $\delta < \delta_0$ as $\delta \to 0$ (3.130) will remain negative and $2\Psi_{\min}\left(\widetilde{\lambda}_\gamma^{\min} - \epsilon, \delta, \rho\right) < 0$.

Having established a negative bound from above and the $\delta_0$ for which it is valid, it remains to show that $n \cdot 2\Psi_{\min}\left(\widetilde{\lambda}_\gamma^{\min} - \epsilon, \delta, \rho\right) \to -\infty$ as $(k,n,N) \to \infty$, which verifies an exponential decay to zero of the bound (3.12) with $n$. This follows from the first term of the right hand side of (3.130) giving a concluding bound $-n \cdot \frac{4}{\sqrt{\gamma^3}}\left(\frac{1}{3} - c_l\right)$. For $\gamma > \gamma_0$ and $\delta < \delta_0$ therefore

$$Prob\left(L(k,n,N;A) > \widetilde{\mathcal{L}}^\gamma(\delta,\rho) + \epsilon\right) \leq poly\left(n, \widetilde{\lambda}_\gamma^{\min} + \epsilon\right) \cdot \exp\left[-\frac{4n}{\sqrt{\gamma^3}}\left(\frac{1}{3} - c_l\right)\right].$$

The right hand side of which goes to zero as $n \to \infty$.

**Part 2:**

$$\begin{aligned}2\Psi_{\min}\left(\widetilde{\lambda}_\gamma^{\min} + \epsilon, \delta, \rho\right) = {} & 2\mathrm{H}(\rho) + (1-\rho)\log\left(\widetilde{\lambda}_\gamma^{\min} + \epsilon\right) \\ & + \rho\log(\rho) - \rho + 1 - \left(\widetilde{\lambda}_\gamma^{\min} + \epsilon\right) + \frac{2}{\delta}\mathrm{H}(\delta\rho),\end{aligned} \tag{3.132}$$

by substituting $\widetilde{\lambda}_\gamma^{\min} + \epsilon$ for $\lambda$ in (3.9). Let $l := 1 - \widetilde{\lambda}_\gamma^{\min}$ and bound the Shannon entropy function from below using the second bound in (3.13) to give

$$2\Psi_{\min}\left(\widetilde{\lambda}_\gamma^{\min} + \epsilon, \delta, \rho\right)$$

$$\begin{aligned}& > 2\left[-\rho\log\rho + \rho - \rho^2\right] + (1-\rho)\log\left[(1-l) + \epsilon\right] + \rho\log\rho - \rho \\ & \quad + 1 - (1-l) - \epsilon + \frac{2}{\delta}\left[-\rho\log(\delta\rho) + \delta\rho - \delta^2\rho^2\right]\end{aligned} \tag{3.133}$$

$$\begin{aligned}& = -2\rho\log\rho + 2\rho - 2\rho^2 + \log(1-l+\epsilon) - \rho\log(1-l+\epsilon) + \rho\log\rho - \rho \\ & \quad + 1 - 1 + l - \epsilon - 2\rho\log(\delta\rho) + 2\rho - 2\delta\rho^2\end{aligned} \tag{3.134}$$

$$\begin{aligned}& = \log(1-l) + \log\left(1 + \frac{\epsilon}{1-l}\right) + l - \epsilon - \rho\log(1-l+\epsilon) + \rho\log\left(\frac{1}{\delta^2\rho^3}\right) \\ & \quad + 3\rho - 2(1+\delta)\rho^2\end{aligned} \tag{3.135}$$

$$\begin{aligned}& > -l - \frac{1}{2}l^2 - \frac{1}{2}l^3 + l + \rho\log\left(\frac{1}{\delta^2\rho^3}\right) + 3\rho + \log(1+\epsilon) - \epsilon \\ & \quad - \rho\log(1-l+\epsilon) - 2(1-\delta)\rho^2\end{aligned} \tag{3.136}$$

$$\begin{aligned}& > -\frac{1}{2}l^2 - \frac{1}{2}l^3 + \rho\log\left(\frac{1}{\delta^2\rho^3}\right) + 3\rho + \epsilon - \frac{1}{2}\epsilon^2 - \epsilon - \rho\log(1-l+\epsilon) \\ & \quad - 2(1-\delta)\rho^2.\end{aligned} \tag{3.137}$$

From (3.133) to (3.134) we expand brackets and simplify. From (3.134) to (3.135) we expand $\log(1-l+\epsilon)$ and simplify. From (3.135) to (3.136) we bound from below $\frac{1}{1-l}$ using (3.46) and using the bound of (3.55) we also bound from below $\log(1-l)$. Then from (3.136) to (3.137) we simplify and bound from below $\log(1+\epsilon)$ using (3.36).

Let $x = 2\rho\log\left(\frac{1}{\delta^2\rho^3}\right) + 6\rho$ which means $l = \sqrt{x} - c_l x$. We simplify (3.137) and replace the second two terms by $\frac{1}{2}x$ and $l$ in the first two terms by $\sqrt{x} - c_l x$ to get

$$
\begin{aligned}
2\Psi_{\min}\left(\widetilde{\lambda}_{\gamma}^{\min}+\epsilon,\delta,\rho\right) > & -\frac{1}{2}\left(\sqrt{x}-c_l x\right)^2 - \frac{1}{2}\left(\sqrt{x}-c_l x\right)^3 + \frac{1}{2}x \\
& -\rho\log\left(1-l+\epsilon\right) - 2(1-\delta)\rho^2 - \frac{1}{2}\epsilon^2 \qquad (3.138)\\
= & -\frac{1}{2}x + c_l x^{3/2} - \frac{1}{2}c_l^2x^2 - \frac{1}{2}x^{3/2} + \frac{3}{2}c_l x^2 - \frac{3}{2}c_l^2 x^{5/2} \\
& + \frac{1}{2}c_l^3x^3 + \frac{1}{2}x - \rho\log\left(1-l+\epsilon\right) - 2(1-\delta)\rho^2 - \frac{1}{2}\epsilon^2 \qquad (3.139)\\
= & \left(c_l - \frac{1}{2}\right)x^{3/2} + \frac{1}{2}c_l\left(3-c_l\right)x^2 - \frac{3}{2}c_l^2x^{5/2} + \frac{1}{2}c_l^3x^3 \\
& -\rho\log\left(1-l+\epsilon\right) - 2(1-\delta)\rho^2 - \frac{1}{2}\epsilon^2. \qquad (3.140)
\end{aligned}
$$

From (3.138) to (3.139) we expand the first two brackets and simplify from (3.139) to (3.140).

The dominant terms that does not go to zero as $\delta \to 0$ are the terms with $x$ and their sum is positive if $c_l \geq 1/2$ and $x < 1$. We established in the earlier parts of this proof of Theorem 3.2.3 that if $\gamma > 4$ we will have $x < 1$ as $\delta \to 0$. Hence we conclude that for fixed $\gamma > \gamma_0 = 4$ and $\epsilon > 0$ there does not exist a $\delta_0$ such that (3.140) is negative and $2\Psi_{\min}\left(\widetilde{\lambda}_{\gamma}^{\min}+\epsilon,\delta,\rho\right) \leq 0$ as $\delta \to 0$. Thus

$$
\begin{aligned}
& \mathit{Prob}\left(L(k,n,N;A) > \widetilde{\mathcal{L}}^{\gamma}(\delta,\rho)-\epsilon\right) \\
& \qquad \leq \mathit{poly}\left(n,\widetilde{\lambda}_{\gamma}^{\min}+\epsilon\right)\cdot\exp\left[2n\Psi_{\min}\left(\widetilde{\lambda}_{\gamma}^{\min}+\epsilon,\delta,\rho\right)\right],
\end{aligned}
$$

and as $n \to \infty$ the right hand side of this does not go to zero.

Now **Part 1** and **Part 2** put together shows that $\widetilde{\mathcal{L}}^{\gamma}(\delta,\rho)$ is also a tight bound of $L(k,n,N;A)$ with overwhelming probability as the sample size grows in the regime prescribed for $\widetilde{\mathcal{L}}^{\gamma}(\delta,\rho)$ in Theorem 3.2.3. □

### 3.6.4 Corollary 3.2.4

*Proof.* We prove Corollary 3.2.4 in two parts, first proving the case for $\widetilde{\mathcal{U}}^{\gamma}(\delta,\rho_\gamma(\delta))$ and then that of $\widetilde{\mathcal{L}}^{\gamma}(\delta,\rho_\gamma(\delta))$.

**Part 1:** From (3.4), for $\rho = \rho_\gamma(\delta) = \frac{1}{\gamma\log\left(\frac{1}{\delta}\right)}$, we have

$$
\widetilde{\mathcal{U}}^{\gamma}(\delta,\rho_\gamma(\delta)) = \sqrt{2\rho\log\left(\frac{1}{\delta^2\rho^3}\right)+6\rho} + c_u\left[2\rho\log\left(\frac{1}{\delta^2\rho^3}\right)+6\rho\right] \qquad (3.141)
$$

$$= \sqrt{2\rho \log\left(\frac{1}{\delta^2\rho^3}\right) + 6\rho + 2c_u\rho \log\left(\frac{1}{\delta^2\rho^3}\right) + 6c_u\rho} \tag{3.142}$$

$$= \sqrt{4\rho \log\left(\frac{1}{\delta}\right) + 6\rho \log\left(\frac{1}{\rho}\right) + 6\rho + 4c_u\rho \log\left(\frac{1}{\delta}\right) + 6c_u\rho \log\left(\frac{1}{\rho}\right) + 6c_u\rho} \tag{3.143}$$

$$= \sqrt{\frac{4}{\gamma} + 6\rho \log\left(\frac{1}{\rho}\right) + 6\rho + \frac{4c_u}{\gamma} + 6c_u\rho \log\left(\frac{1}{\rho}\right) + 6c_u\rho}. \tag{3.144}$$

From (3.141) to (3.142) we expand the square brackets while from (3.142) to (3.143) we separate the terms explicitly involving $\delta$ from the rest. From (3.143) to (3.144) we substitute $1/\left[\gamma \log(1/\delta)\right]$ for $\rho$ in the terms explicitly involving $\delta$ and simplify.

Now using the fact that $\lim_{\delta\to 0} \rho \log(1/\rho) = 0$ and $\lim_{\delta\to 0} \rho = 0$ we have

$$\lim_{\delta\to 0} \widetilde{\mathfrak{U}}^{\gamma}(\delta, \rho_\gamma(\delta)) = \frac{2}{\sqrt{\gamma}} + \frac{4c_u}{\gamma},$$

hence concluding the proof for $\widetilde{\mathfrak{U}}^{\gamma}(\delta, \rho_\gamma(\delta))$.

**Part 2:** From (3.5), for $\rho = \rho_\gamma(\delta) = \frac{1}{\gamma \log\left(\frac{1}{\delta}\right)}$, we have

$$\widetilde{\mathcal{L}}^{\gamma}(\delta, \rho_\gamma(\delta)) = \sqrt{2\rho \log\left(\frac{1}{\delta^2\rho^3}\right) + 6\rho} - c_l \left[2\rho \log\left(\frac{1}{\delta^2\rho^3}\right) + 6\rho\right] \tag{3.145}$$

$$= \sqrt{2\rho \log\left(\frac{1}{\delta^2\rho^3}\right) + 6\rho} - 2c_l\rho \log\left(\frac{1}{\delta^2\rho^3}\right) - 6c_l\rho \tag{3.146}$$

$$= \sqrt{4\rho \log\left(\frac{1}{\delta}\right) + 6\rho \log\left(\frac{1}{\rho}\right) + 6\rho} - 4c_l\rho \log\left(\frac{1}{\delta}\right) - 6c_l\rho \log\left(\frac{1}{\rho}\right) - 6c_l\rho \tag{3.147}$$

$$= \sqrt{\frac{4}{\gamma} + 6\rho \log\left(\frac{1}{\rho}\right) + 6\rho} - \frac{4c_l}{\gamma} - 6c_l\rho \log\left(\frac{1}{\rho}\right) - 6c_l\rho. \tag{3.148}$$

From (3.145) to (3.146) we expand the square brackets while from (3.146) to (3.147) we separate the terms explicitly involving $\delta$ from the rest. Then from (3.147) to (3.148) we substitute $1/\left[\gamma \log(1/\delta)\right]$ for $\rho$ in the terms explicitly involving $\delta$ and simplify.

Now using the fact that $\lim_{\delta\to 0} \rho \log(1/\rho) = 0$ and $\lim_{\delta\to 0} \rho = 0$ we have

$$\lim_{\delta\to 0} \widetilde{\mathcal{L}}^{\gamma}(\delta, \rho_\gamma(\delta)) = \frac{2}{\sqrt{\gamma}} - \frac{4c_l}{\gamma},$$

hence concluding the proof for $\widetilde{\mathfrak{U}}^{\gamma}(\delta, \rho_\gamma(\delta))$.

**Part 1** and **Part 2** combined concludes the proof for Corollary 3.2.4. □

# Chapter 4

# Sparse Matrices and Expander Graphs, with Application to Compressed Sensing

## 4.1 Introduction

There are computational advantages from using sparse matrices and recently, recovery guarantees for using non-mean zero sparse matrices in compressed sensing has been derived in the form of the $\ell_1$-norm restricted isometry constants (RIC$_1$) [15]. This chapter is about work in this direction. We consider random sparse matrices that are adjacency matrices of lossless expander graphs and present quantitative guarantees on the probabilistic construction of lossless expander graphs by providing a bound on the tail probability of the size of the *set of neighbours* of a randomly generated left-degree bipartite graph. Consequently, we provide a bound on the tail probability of the *expansion* of the graph. Furthermore, we present quantitative guarantees for randomly generated non-mean zero sparse binary matrices to be adjacency matrices of expander graphs. We also derive the first phase transitions showing regions in parameter space depicting when a left-regular bipartite graph with a given set of parameters is guaranteed with high probability to be a lossless expander. The key innovation in this work is the use of a novel technique of *dyadic splitting of sets* to derive our bound.

Several compressed sensing algorithms have been designed for sparse matrices [149, 15, 16, 80]. In an effort to quantitatively compare the performance guarantees of these proposed algorithms we derive sampling theorems, presented as phase transitions, comparing performance guarantees for some of these algorithms as well as the more traditional $\ell_1$-minimization compressed sensing formulation. We also show how favourably $\ell_1$-minimization performance guarantees for such sparse matrices compared to what $\ell_2$-norm restricted isometry constants

($\text{RIC}_2$) analysis yields for the dense Gaussian matrices. For this comparison, we used sampling theorems and phase transitions from related work by Blanchard et. al. [20] that provided such theorems for dense Gaussian matrices based on $\text{RIC}_2$ analysis.

The outline of the chapter [1] goes as follows: In Section 4.2 we present our main results in Subsection 4.2.1 and we discuss $\text{RIC}_1$ and its implication for compressed sensing and expander graphs in Subsection 4.2.2. In Section 4.3 we show empirical data to validate our main results and also present lemmas (and their proofs) that are key to the proof of the main theorem, Theorem 4.2.4. In Section 4.4 we discuss restricted isometry constants and compressed sensing algorithms. In Section 4.5 we prove the mains results, that is Theorem 4.2.4 and 4.2.6 and the corollaries in Subsections 4.2.1, 4.2.2 and 4.3.1.

## 4.2 Sparse Matrices and Expander Graphs

Here we present our main results in Section 4.2.1 in the form of Theorem 4.2.4 and Corollary 4.2.5. In Section 4.2.2 we discuss $\text{RIC}_1$ and its implication for compressed sensing and existence of expander graphs, leading to two sampling theorems in Corollaries 4.2.7 and 4.2.8.

### 4.2.1 Main Results

Our main results are about a class of sparse matrices coming from lossless expander graphs, a class which include non-mean zero matrices. We start by defining the class of matrices we consider and the concept of a *set of neighbours* used in the derivation of the main results.

**Definition 4.2.1.** *Let $A$ be an $n \times N$ matrix with $d$ nonzeros in each column. We refer to $A$ as a random*

1. *sparse expander (SE) if every nonzero has value* $1$
2. *sparse signed expander (SSE) if every nonzero has value from* $\{-1, 1\}$

*and the support set of the $d$ nonzeros per column are drawn uniformly at random, with each column drawn independently.*

SE matrices are adjacency matrices of lossless $(k, d, \epsilon)$-expander graphs while SSE matrices have random sign patterns in the nonzeros of an adjacency matrix of a lossless $(k, d, \epsilon)$-expander graph. If $A$ is either an SE or SSE it will have only $d$ nonzeros per column and since we fix $d \ll n$, $A$ is therefore "vanishingly sparse." To aid translation between the terminology of graph theory and linear algebra we define the *set of neighbours* in both notations.

**Definition 4.2.2.** *Consider a bipartite graph $G(U, V, E)$ where $E$ is the set of edges and $e_{ij} = (x_i, y_j)$ is the edge that connects vertex $x_i$ to vertex $y_j$. For a given set of left vertices $S \subset U$*

[1] Material in this chapter has been prepared for publication and in preprint [8] in a joint authorship with J. Tanner whose permission has been obtained for the inclusion of the material.

*its set of neighbours is* $\Gamma(S) = \{y_j | x_i \in S \text{ and } e_{ij} \in E\}$*. In terms of the adjacency matrix,* $A$*, of* $G(U, V, E)$ *the set of neighbours of* $A_S$ *for* $|S| = s$*, denoted by* $A_s$*, is the set of rows in* $A_S$ *with at least one nonzero.*

**Definition 4.2.3.** *Using Definition 4.2.2, the expansion of the graph is given by the ratio* $|\Gamma(S)|/|S|$*, or equivalently,* $|A_s|/s$*.*

By the definition of a lossless expander, Definition 1.3.1, we need $|\Gamma(S)|$ to be large for every small $S \subset U$. In terms of the class of matrices defined by Definition 4.2.1, for every $A_S$ we want to have $|A_s|$ as close to $n$ as possible, where $n$ is the number of rows. Henceforth, we will only use the linear algebra notation $A_s$ which is equivalent to $\Gamma(S)$. Note that $|A_s|$ is a random variable depending on the draw of the set of columns, $S$, for each fixed $A$. Therefore, we can ask what is the probability that $|A_s|$ is not greater than $a_s$, in particular where $a_s$ is smaller than the expected value of $|A_s|$. This is the question that Theorem 4.2.4 seeks to answer. We then use this theorem with RIC$_1$ to deduce the corollaries that follow which are about the probabilistic construction of expander graphs, the matrices we consider, and sampling theorems for some selected compressed sensing algorithms.

**Theorem 4.2.4.** *For fixed* $s, n, N$ *and* $d$*, let an* $n \times N$ *matrix* $A$ *be drawn from either of the classes of matrices defined in Definition 4.2.1. Then*

$$\mathit{Prob}\left(|A_s| \leq a_s\right) < p_{max}(s,d) \cdot \exp\left[n \cdot \Psi\left(a_s, \ldots, a_2, d\right)\right] \tag{4.1}$$

*where*

$$p_{max}(s,d) = \frac{2}{25\sqrt{2\pi s^3 d^3}}, \tag{4.2}$$

*and* $\Psi\left(a_s, \ldots, a_2, d\right)$ *is given by*

$$\frac{1}{n}\left[\sum_{i=1}^{\lceil s/2 \rceil} \frac{s}{2i}\left(a_i \cdot H\left(\frac{a_{2i}-a_i}{a_i}\right) + (n-a_i)\cdot H\left(\frac{a_{2i}-a_i}{n-a_i}\right) - n \cdot H\left(\frac{a_i}{n}\right)\right) + 3s\log(5d)\right] \tag{4.3}$$

*where* $a_1 := d$ *and* $H(\cdot)$ *is the Shannon Entropy function with base* $e$ *logarithms given in* (1.2)*. If no restriction is imposed on* $a_s$ *then the* $a_i$ *for* $i > 1$ *take on their expected value* $\hat{a}_i$ *given by*

$$\hat{a}_{2i} = \hat{a}_i\left(2 - \frac{\hat{a}_i}{n}\right) \quad \mathit{for} \quad i = 1, 2, 4, \ldots, \lceil s/2 \rceil. \tag{4.4}$$

*If* $a_s$ *is restricted to be less than* $\hat{a}_s$*, then the* $a_i$ *for* $i > 1$ *are the unique solutions to the following polynomial system*

$$a_{2i}^3 - 2a_i a_{2i}^2 + 2a_i^2 a_{2i} - a_i^2 a_{4i} = 0 \; \mathit{for} \;\; i = 1, 2, \ldots, \lceil s/4 \rceil \tag{4.5}$$

*with* $a_{2i} \geq a_i$ *for each* $i$*.*

**Corollary 4.2.5.** *For fixed $s, n, N, d$ and $0 < \epsilon < 1/2$, let an $n \times N$ matrix $A$ be drawn from the class of matrices defined in Definition 4.2.1, then*

$$Prob\left(\|A_S x\|_1 \leq (1-2\epsilon)d\|x\|_1\right) < p_{max}(s,d)\exp\left[n \cdot \Psi\left(s,d,\epsilon\right)\right] \tag{4.6}$$

*where $\Psi\left(s,d,\epsilon\right) = \Psi\left(a_s,\ldots,a_2,d\right)$ in* (4.3) *with $a_s = (1-\epsilon)ds$ and $p_{max}(s,d)$ is the polynomial in* (4.2).

Theorem 4.2.4 and Corollary 4.2.5 allow us to calculate $s, n, N, d, \epsilon$ where the probability of the probabilistic constructions in Definition 4.2.1 not being a lossless $(s, d, \epsilon)$-expander is exponentially small. For moderate values of $\epsilon$ this allows us to make quantitative sampling theorems for some compressed sensing reconstruction algorithms.

### 4.2.2 Implications of $\mathrm{RIC}_1$ for Compressed Sensing and Expanders

The reader is reminded that in compressed sensing, and by extension in sparse approximation, we observe the effect of the application of a matrix to a vector of interest and we endeavour to recover this vector of interest by exploiting the inherent simplicity in this vector. We are able to give guarantees on the quality of the reconstructed vector from $A$ and $y$ from a variety of reconstruction algorithms. One of these guarantees is a bound on the approximation error between our recovered vector, say $\hat{x}$, and the original vector by the best $k$-term representation error i.e. $\|x - \hat{x}\|_1 \leq C\|x - x_k\|_1$ with constant $C > 0$ where $x_k$ is the optimal $k$-term representation for $x$. This is possible if $A$ has small $\mathrm{RIC}_1$, in other words $A$ satisfies the $\ell_1$-norm restricted isometry property (RIP-1), introduced by Berinde et. al. in [15] and defined in Definition 1.1.4.

For computational purposes it is preferable to have $A$ sparse, but little quantitative information on $\overline{L}(k, n, N; A)$ has been available for large sparse rectangular matrices. Berinde et. al. in [15] showed that scaled adjacency matrices of lossless expander graphs (i.e. scaled SE matrices) satisfy RIP-1. We extend this equivalence to random non-mean zero binary matrices with fixed number of nonzeros in each column where the nonzeros have random signs, i.e. SSE matrices. Theorem 4.2.6 states this for the two sets of matrices and its proof is presented in Section 4.5.3.

**Theorem 4.2.6.** *If an $n \times N$ matrix $A$ is either SE or SSE defined in Definition 4.2.1, then $\frac{1}{d}A$ satisfies RIP-1 with $\overline{L}(k, n, N; A) = 2\epsilon$.*

Based on Theorem 4.2.6 which guarantees RIP-1, (1.10), for the class of matrices in Definition 4.2.1, we give a bound, in Corollary 4.2.7, for the probability that a random draw of a matrix with $d$ 1s or ±1s in each column fails to satisfy the lower bound of RIP-1 and hence fails to come from the class of matrices given in Definition 4.2.1. Note that with these matrices the upper RIC$_1$ is always satisfied, i.e., $\|Ax\|_1 \leq d\|x\|_1$ always holds. In addition to Theorem 4.2.6, Corollary 4.2.7 follows from Theorem 4.2.4 and Corollary 4.2.5.

**Corollary 4.2.7.** *Considering RIP-1, if $A$ is drawn from the class of matrices in Definition 4.2.1 and any $k$-sparse vector $x$ with $k, n, N$ and $0 < \epsilon < 1/2$ fixed, then*

$$\textit{Prob}\left(\|Ax\|_1 \leq (1-2\epsilon)d\|x\|_1\right) < p'_{max}(N,k,d) \times \exp\left[N \cdot \Psi_{net}\left(k,n,N;d,\epsilon\right)\right] \tag{4.7}$$

*where $p'_{max}(N,k,d)$ and $\Psi_{net}\left(k,n,N;d,\epsilon\right)$ are given by*

$$p'_{max}(N,k,d) = \frac{1}{16\pi k\sqrt{d^3\left(1-\frac{k}{N}\right)}}, \tag{4.8}$$

$$\Psi_{net}\left(k,n,N;d,\epsilon\right) = H\left(\frac{k}{N}\right) + \frac{n}{N}\Psi\left(k,d,\epsilon\right), \tag{4.9}$$

*with $\Psi\left(k,d,\epsilon\right)$ defined in Corollary 4.2.5.*

Furthermore, the following corollary is a consequence of Corollary 4.2.7 and it is a sampling theorem on the existence of lossless expander graphs. The proof of Corollaries 4.2.7 and 4.2.8 are presented in Section 4.5.4.

**Corollary 4.2.8.** *Consider $0 < \epsilon < 1/2$ and $d$ fixed. If $A$ is drawn from the class of matrices in Definition 4.2.1 and any $x$ drawn from $\chi^N$ with $(k,n,N) \to \infty$ while $k/n \to \rho \in (0,1)$ and $n/N \to \delta \in (0,1)$ then for $\rho < (1-\gamma)\rho^{exp}(\delta;d,\epsilon)$ and $\gamma > 0$*

$$\textit{Prob}\left(\|Ax\|_1 \geq (1-2\epsilon)d\|x\|_1\right) \to 1 \tag{4.10}$$

*exponentially in $n$, where $\rho^{exp}(\delta;d,\epsilon)$ is the largest limiting value of $k/n$ for which*

$$H\left(\frac{k}{N}\right) + \frac{n}{N}\Psi\left(k,d,\epsilon\right) = 0, \tag{4.11}$$

*with $\Psi\left(k,d,\epsilon\right)$ defined in Corollary 4.2.5.*

## 4.3 Discussion and Derivation of the Main Results

We present the method used to derive the main results and discuss the validity and implications of the method. We start by presenting in the next subsection, Section 4.3.1, numerical results that support the claims of the main results in Sections 4.2.1 and 4.2.2. This is followed in Section 4.3 with lemmas, propositions and corollaries and their proofs.

### 4.3.1 Discussion of Main Results

Theorem 4.2.4 gives a bound on the probability that the cardinality of a union of $k$ sets each with $d$ elements is less than $a_k$. The left panel of Figure 4.1 shows plots of values of $a_k$ (size of set of neighbours) for different $k$ taken over 500 realizations (in blue), superimposed on these plots is the mean value of $a_k$ (in red) and the $\hat{a}_k$ in green. Similarly, the right panel of Figure 4.1 also shows values of $a_k/k$ (the graph expansion) also taken over 500 realizations.

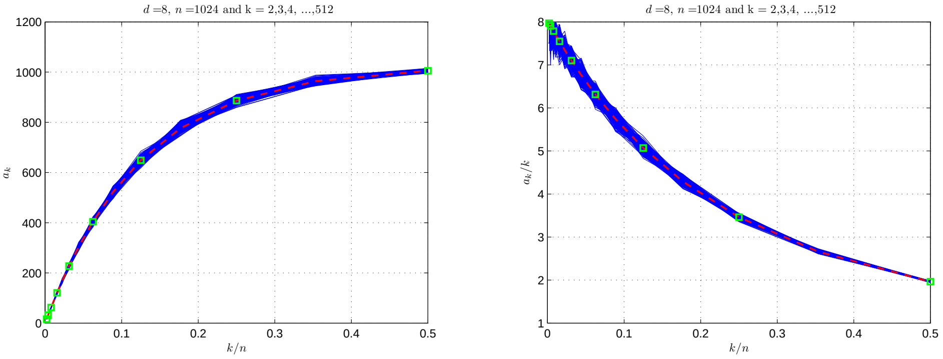

Figure 4.1: For fixed $d = 8$ and $n = 2^{10}$, over 500 realizations, *left panel:* plots (in blue) the cardinalities of the index sets of nonzeros in a given number of set sizes, $k$. The dotted red curve is mean of the simulations and the green squares are the $\hat{a}_k$; *right panel:* plots (in blue) the graph expansion for a given input set size $k$. The dotted red curve is mean of the simulations and the green squares are the $\hat{a}_k/k$.

Theorem 4.2.4 also claims that the $\hat{a}_s$ are the expected values of the cardinalities of the union of $s$ sets. We give a sketch of its proof in Section 4.3.2 in terms of the maximum likelihood and empirically illustrate the accuracy of the result in the left panel of Figure 4.2 where we show the relative error between $\hat{a}_k$ and the mean values of the $a_k, \bar{a}_k$, realized over 500 runs, to be less than $10^{-3}$. The right panel of Figure 4.2 shows representative values of $a_i$ from (4.5) for $a_k := (1-\epsilon)\hat{a}_k$ as a function of $\epsilon$ for $d = 8$, $k = 2 \times 10^3$, and $n = 2^{20}$. Each of the $a_i$ decrease smoothly towards $d$, but with $a_i$ for smaller values of $i$ varying less than for larger values of $i$.

For fixed $0 < \epsilon < 1/2$ and for small but fixed $d$, $\rho^{exp}(\delta; d, \epsilon)$ in Corollary 4.2.8 is a function of $\delta$ for each $d$ and $\epsilon$, is a phase transition function in the $(\delta, \rho)$ plane. Below the curve of $\rho^{exp}(\delta; d, \epsilon)$ the probability in (4.10) goes to one exponentially in $n$ as the problem size grows. That is if $A$ is drawn at random with $d$ 1s or $d$ ± 1s in each column and having parameters $(k, n, N)$ that fall below the curve of $\rho^{exp}(\delta; d, \epsilon)$ then we say it is from the class of matrices in Definition 4.2.1 with probability approaching one exponentially in $n$. In terms of $|\Gamma(X)|$ for $X \subset U$ and $|X| \leq k$, Corollary 4.2.8 say that the probability $|\Gamma(X)| \geq (1-\epsilon)dk$ goes to one exponentially in $n$ if the parameters of our graph lies in the region below $\rho^{exp}(\delta; d, \epsilon)$. This implies that if we draw a random bipartite graphs that has parameters in the region below the curve of $\rho^{exp}(\delta; d, \epsilon)$ then with probability approaching one exponentially in $n$ that graph is a lossless $(k, d, \epsilon)$-expander.

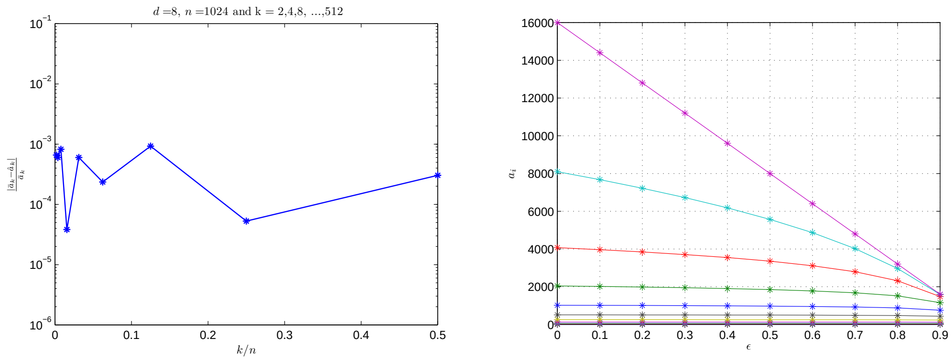

Figure 4.2: *Left panel:* For fixed $d = 8$ and $n = 2^{10}$, over 500 realizations the relative error between the mean values of $a_k$ (referred to as $\bar{a}_k$) and the $\hat{a}_k$ from Equation (4.4) of Theorem 4.2.4. *Right panel:* Values of $a_i$ as a function of $\epsilon \in [0, 1)$ for $a_k := (1 - \epsilon)\hat{a}_k$ with $d = 8$, $k = 2 \times 10^3$ and $n = 2^{20}$. For this choice of $d, k, n$ there are twelve levels of dyadic splits resulting in $a_i$ for $i = 2^j$ for $j = 0, \ldots, \lceil \log_2 k \rceil = 12$. The highest curve corresponds to $a_i$ for $i = 2^{12}$, the next highest curve corresponds to $i = 2^{11}$, and continuing in decreasing magnitude with decreasing subscript values.

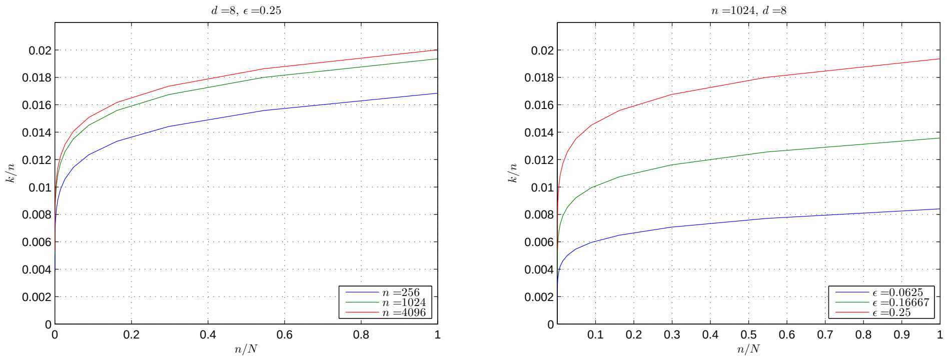

Figure 4.3: Phase transition plots of $\rho^{exp}(\delta; d, \epsilon)$ for fixed $d = 8$, *left panel:* and fixed $\epsilon = 1/4$ with $n$ varied; *right panel:* and fixed $n = 2^{10}$ with $\epsilon$ varied.

The left panel of Figure 4.3 shows a plot of what $\rho^{exp}(\delta; d, \epsilon)$ converge to for different values of $n$ with $\epsilon$ and $d$ fixed; while the right panel of Figure 4.3 shows plots of what $\rho^{exp}(\delta; d, \epsilon)$ converge to for different values of $\epsilon$ with $n$ and $d$ fixed. Furthermore, the left panel of Figure 4.4 shows a plot of what $\rho^{exp}(\delta; d, \epsilon)$ converge to for different values of $d$ with $\epsilon$ and $n$ fixed. It is interesting to note how increasing $d$ increases the phase transition up to a point then it decreases the phase transition. Essentially beyond $d = 16$ there is no gain in increasing $d$. This vindicates the use of small $d$ in most of the numerical simulations involving the class of matrices considered here. Note the vanishing sparsity as the problem size $(k, n, N)$ grows while $d$ is fixed to a small value of 8. In their GPU implementation [21] Blanchard and Tanner observed that SSE with $d = 7$ has a phase transition for numerous sparse approximation algorithms that is consistent with dense Gaussian matrices, but with dramatically faster implementation.

As afore mentioned Corollary 4.2.8 follows from Theorem 4.2.4, alternatively Corollary 4.2.8 can be arrived at based on probabilistic constructions of expander graphs given by Proposition

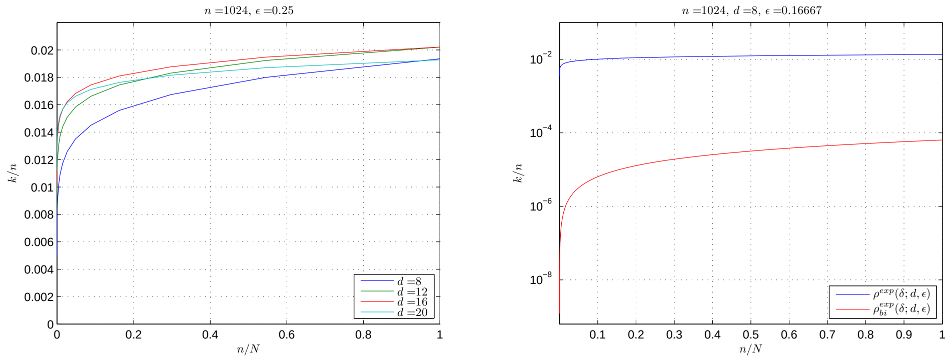

Figure 4.4: *Left panel:* Phase transition plots of $\rho^{exp}(\delta; d, \epsilon)$ for fixed $\epsilon = 1/6$ and $n = 2^{10}$ with $d$ varied. *Right panel:* A comparison of the phase transition, $\rho^{exp}$, based on Theorem 4.2.4 to $\rho_{bi}^{exp}$ derived using the construction based on Corollary 4.3.2.

4.3.1 below. This proposition and its proof can be traced back to Pinsker in [112] but more recent proofs can be found in [14, 41].

**Proposition 4.3.1.** *For any $N/2 \geq k \geq 1$, $\epsilon > 0$ there exists a lossless $(k, d, \epsilon)$-expander with*

$$d = \mathcal{O}\left(\log\left(N/k\right)/\epsilon\right) \quad \text{and} \quad n = \mathcal{O}\left(k \log\left(N/k\right)/\epsilon^2\right).$$

To put our results in perspective, we compare them to the alternative construction in [14] which led to Corollary 4.3.2, whose proof is given in Section 4.5.4. The right panel of Figure 4.4 compares the phase transitions resulting from our construction to that presented in [14], but we must point out however, that the proof in [14] was not aimed for a tight bound.

**Corollary 4.3.2.** *Consider a bipartite graph $G(U, V, E)$ with left vertices $|U| = N$, right vertices $|V| = n$ and left degree $d$. Fix $0 < \epsilon < 1/2$ and $d$, as $(k, n, N) \to \infty$ while $k/n \to \rho \in (0, 1)$ and $n/N \to \delta \in (0, 1)$ then for $\rho < (1-\gamma)\rho_{bi}^{exp}(\delta; d, \epsilon)$ and $\gamma > 0$*

$$\text{Prob}\left(G \text{ fails to be an expander}\right) \to 0 \tag{4.12}$$

*exponentially in $n$, where $\rho_{bi}^{exp}(\delta; d, \epsilon)$ is the largest limiting value of $k/n$ for which*

$$\Psi\left(k, n, N; d, \epsilon\right) = 0 \tag{4.13}$$

*with* $\Psi\left(k, n, N; d, \epsilon\right) = H\left(\frac{k}{N}\right) + \frac{dk}{N} H\left(\epsilon\right) + \frac{\epsilon dk}{N} \log\left(\frac{dk}{n}\right).$

### 4.3.2 Key Lemmas

The following set of lemmas, propositions and corollaries form the building blocks of the proof of our main results to be presented in Section 4.5.

For one fixed set of columns of $A$, denoted $A_S$, the probability in (4.1) can be understood as the cardinality of the unions of indices of nonzeros in the columns. Our analysis of this probability follows from a nested unions of subsets using a *dyadic splitting* technique. Given a starting set of columns we recursively split the number of columns from this set and the resulting sets into two sets of cardinality of the ceiling and floor of the cardinality of their union until a level when the cardinalities are at most two. Resulting from this type of splitting is a binary tree where the size of each child is either the ceiling or the floor of the size of its parent set. The probability of interest becomes a product of the probabilities involving all the children from the dyadic splitting of $A_s$.

The computation of the probability in (4.1) involves the computation of the probability of the cardinality of the intersection of two sets. This probability is given by Lemma 4.3.3 and Corollary 4.3.4 below.

**Lemma 4.3.3.** *Let $B,\ B_1,\ B_2 \subset [n]$ where $|B_1| = b_1$, $|B_2| = b_2$, $B = B_1 \cup B_2$ and $|B| = b$. Also let $B_1$ and $B_2$ be drawn uniformly at random, independent of each other, and define $P_n(b, b_1, b_2) := Prob(|B_1 \cap B_2| = b_1 + b_2 - b)$, then*

$$P_n(b, b_1, b_2) = \binom{b_1}{b_1 + b_2 - b}\binom{n - b_1}{b - b_1}\binom{n}{b_2}^{-1}. \tag{4.14}$$

*Proof.* Given $B_1, B_2 \subset [n]$ where $|B_1| = b_1$ and $|B_2| = b_2$ are drawn uniformly at random, independent of each other, we calculate $\text{Prob}(|B_1 \cap B_2| = z)$ where $z = b_1 + b_2 - b$. Without loss of generality consider drawing $B_1$ first, then the probability that the draw of $B_2$ intersecting $B_1$ will have cardinality $z$, i.e. $\text{Prob}(|B_1 \cap B_2| = z)$, is the size of the event of drawing $B_2$ intersecting $B_1$ by $z$ divided by the size of the sample space of drawing $B_2$ from $[n]$, which are given by $\binom{b_1}{z} \cdot \binom{n-b_1}{b_2 - z}$ and $\binom{n}{b_2}$ respectively. Rewriting the division as a product with the divisor raised to a negative power and replacing $z$ by $b_1 + b_2 - b$ gives (4.14). □

**Corollary 4.3.4.** *If two sets, $B_1, B_2 \subset [n]$ are drawn uniformly at random, independent of each other, and $B = B_1 \cup B_2$*

$$Prob(|B| = b) = P_n(b, b_1, b_2) \cdot Prob(|B_1| = b_1) \cdot Prob(|B_2| = b_2) \tag{4.15}$$

*Proof.* $\text{Prob}(|B| = b) = \text{Prob}(|B_1 \cup B_2| = b)$ by definition. As a consequence of the inclusion-exclusion principle

$$\text{Prob}(|B_1 \cup B_2| = b) = \text{Prob}(|B_1 \cap B_2| = b_1 + b_2 - b) \cdot \prod_{j=1}^{2} \text{Prob}(|B_j| = b_j). \tag{4.16}$$

We use Lemma 4.3.3 to replace $\text{Prob}(|B_1 \cap B_2| = b_1 + b_2 - b)$ in (4.16) by $\text{P}_n(b, b_1, b_2)$ leading to the required result. □

In the binary tree resulting from our dyadic splitting scheme the number of columns in the two children of a parent node is the ceiling and the floor of half of the number of columns of the parent node. At each level of the split the number of columns of the children of that level differ by one. The enumeration of these two quantities at each level of the splitting process is necessary in the computation of the probability of (4.1). We state and prove what we refer to a *dyadic splitting lemma*, Lemma 4.3.5, which we later use to enumerate these two quantities - the sizes (number of columns) of the children and the number of children with a given size at each level of the split.

**Lemma 4.3.5.** *Let $S$ be an index set of cardinality $s$. For any level $j$ of the dyadic splitting, $j = 0, \ldots, \lceil \log_2 s \rceil - 1$, the set $S$ is decomposed into disjoint sets each having cardinality $Q_j = \left\lceil \frac{s}{2^j} \right\rceil$ or $R_j = Q_j - 1$. Let $q_j$ sets have cardinality $Q_j$ and $r_j$ sets have cardinality $R_j$, then*

$$q_j = s - 2^j \cdot \left\lceil \frac{s}{2^j} \right\rceil + 2^j, \quad \textit{and} \quad r_j = 2^j - q_j. \tag{4.17}$$

*Proof.* At every node on the binary tree the children have either of two sizes (number of columns) of the floor and ceiling of half the sizes of there parents and these sizes differ at most by 1, that is at level $j$ of the splitting we have at most 2 different sizes. We define these sizes, $Q_j$ and $R_j$, in terms of two arbitrary integers, $m_1$ and $m_2$, as follows.

$$Q_j = \frac{s}{2^j} + \frac{m_1}{2^j} \quad \text{and} \quad R_j = \frac{s}{2^j} + \frac{m_2}{2^j}. \tag{4.18}$$

Because of the nature of our splitting scheme we have $R_j = Q_j - 1$ which implies that $m_1$ and $m_2$ must satisfy the relation

$$\frac{m_1 - m_2}{2^j} = 1. \tag{4.19}$$

Now let $q_j$ and $r_j$ be the number of children with $Q_j$ and $R_j$ number of columns respectively. Therefore,

$$q_j + r_j = 2^j. \tag{4.20}$$

At each level $j$ of the splitting the following condition must be satisfied

$$q_j \cdot Q_j + r_j \cdot R_j = s. \tag{4.21}$$

To find $m_1$, $m_2$, $q_j$ and $r_j$, from (4.18) we substitute for $Q_j$ and $R_j$ in (4.21) to have

$$q_j \cdot \left( \frac{s}{2^j} + \frac{m_1}{2^j} \right) + r_j \cdot \left( \frac{s}{2^j} + \frac{m_2}{2^j} \right) = s, \tag{4.22}$$

$$2^{-j} q_j s + 2^{-j} q_j m_1 + 2^{-j} r_j s + 2^{-j} r_j m_2 = s, \tag{4.23}$$

$$2^{-j} \left( q_j + r_j \right) s + 2^{-j} \left( q_j m_1 + r_j m_2 \right) = s, \tag{4.24}$$

$$s + 2^{-j} \left( q_j m_1 + r_j m_2 \right) = s. \tag{4.25}$$

We expand the brackets from (4.22) to (4.23) and simplify from (4.23) to (4.24). We simplify the first term of (4.24) using (4.20) to get (4.25). Now we simplify this to get (4.26) below.

$$q_j m_1 + r_j m_2 = 0. \tag{4.26}$$

Equation (4.19) yields

$$m_1 = m_2 + 2^j. \tag{4.27}$$

Substituting this in (4.26) yields

$$q_j \left(m_2 + 2^j\right) + r_j m_2 = 0, \tag{4.28}$$

$$\left(q_j + r_j\right) m_2 + 2^j q_j = 0, \tag{4.29}$$

$$2^j \left(q_j + m_2\right) = 0. \tag{4.30}$$

From (4.28) to (4.29) we expand the brackets and rearrange the terms and use (4.20) to simplify to (4.30). Using (4.30) and (4.27) respectively we have

$$m_2 = -q_j \quad \text{and} \quad m_1 = 2^j - q_j = r_j. \tag{4.31}$$

Substituting this in (4.18) we have

$$Q_j = \frac{s - q_j}{2^j} + 1 \quad \text{and} \quad R_j = \frac{s - q_j}{2^j}. \tag{4.32}$$

Equating this value of $Q_j$ to its defined value in the statement of the lemma gives

$$\frac{s - q_j}{2^j} + 1 = \left\lceil \frac{s}{2^j} \right\rceil \quad \Rightarrow \quad q_j = s - 2^j \cdot \left\lceil \frac{s}{2^j} \right\rceil + 2^j. \tag{4.33}$$

Therefore, from (4.31) we use (4.33) to have

$$r_j = 2^j - q_j \quad \Rightarrow \quad r_j = 2^j \cdot \left\lceil \frac{s}{2^j} \right\rceil - s, \tag{4.34}$$

which concludes the proof. □

The bound in (4.1) is derived using a large deviation analysis of the nested probabilities which follow from the dyadic splitting in Corollary 4.3.4. The large deviation analysis of (4.14) at each stage involves its large deviation exponent $\psi_n(\cdot)$, which follows from Stirling's inequality bounds on the combinatorial product of (4.14). Lemma 4.3.6 establishes a few properties of $\psi_n(\cdot)$ while Lemma 4.3.7 shows how the various $\psi_n(\cdot)$'s at a given dyadic splitting level can be combined into a relatively simple expression.

**Lemma 4.3.6.** *Define*

$$\psi_n(x,y,z) := y \cdot H\left(\frac{x-z}{y}\right) - n \cdot H\left(\frac{z}{n}\right) + (n-y) \cdot H\left(\frac{x-y}{n-y}\right), \tag{4.35}$$

*then for $n > x > y$ we have that*

$$\text{for } y > z \quad \psi_n(x,y,y) \leq \psi_n(x,y,z) \leq \psi_n(x,z,z); \tag{4.36}$$

$$\text{for } x > z \quad \psi_n(x,y,y) > \psi_n(z,y,y); \tag{4.37}$$

$$\text{for } 1/2 < \alpha \leq 1 \quad \psi_n(x,y,y) < \psi_n(\alpha x, \alpha y, \alpha y). \tag{4.38}$$

*Proof.* We start with Property (4.36) and first show that the left inequality holds. If we substitute $y$ for $z$ in (4.35) with $y > z$ we reduce the first and last terms of (4.35) while we increase the middle term of (4.35) which makes $\psi_n(x,y,y) \leq \psi_n(x,y,z)$. For second inequality we replace $y$ by $z$ in (4.35) with $y > z$ we increase the first and the last terms of (4.35) and reduce the middle term which makes $\psi_n(x,y,z) \leq \psi_n(x,z,z)$. This concludes the proof for (4.36).

Property (4.37) states that for fixed $y$, $\psi_n(x,y,y)$ is monotonically increasing in its first argument. To prove (4.37) we again use the condition $n > x > y$ to ensure that $\mathrm{H}(p)$ increases monotonically with $p$, which implies that the first and last terms of (4.35) increase with $x$ for fixed $y$ while the second term remains constant.

Property (4.38) means that $\psi_n(x,y,y)$ is monotonically decreasing in $x$ and $y$. For the proof we show that for $1/2 < \alpha \leq 1$ the difference $\psi_n(\alpha x, \alpha y, \alpha y) - \psi_n(x,y,y) > 0$. Using (4.35) we write out clearly what the difference, $\psi_n(\alpha x, \alpha y, \alpha y) - \psi_n(x,y,y)$, is as follows.

$$\begin{aligned}
&\alpha y \cdot \mathrm{H}\left(\frac{\alpha x - \alpha y}{\alpha y}\right) + (n - \alpha y) \cdot \mathrm{H}\left(\frac{\alpha x - \alpha y}{n - \alpha y}\right) - n \cdot \mathrm{H}\left(\frac{\alpha y}{n}\right) \\
&\quad - y \cdot \mathrm{H}\left(\frac{x-y}{y}\right) - (n-y) \cdot \mathrm{H}\left(\frac{x-y}{n-y}\right) + n \cdot \mathrm{H}\left(\frac{y}{n}\right) && (4.39) \\
&= \alpha y \cdot \mathrm{H}\left(\frac{x-y}{y}\right) + n \cdot \mathrm{H}\left(\frac{\alpha x - \alpha y}{n - \alpha y}\right) - \alpha y \cdot \mathrm{H}\left(\frac{\alpha x - \alpha y}{n - \alpha y}\right) - n \cdot \mathrm{H}\left(\frac{\alpha y}{n}\right) \\
&\quad - y \cdot \mathrm{H}\left(\frac{x-y}{y}\right) - n \cdot \mathrm{H}\left(\frac{x-y}{n-y}\right) + y \cdot \mathrm{H}\left(\frac{x-y}{n-y}\right) + n \cdot \mathrm{H}\left(\frac{y}{n}\right) && (4.40) \\
&= \alpha y \cdot \mathrm{H}\left(\frac{x-y}{y}\right) - \alpha y \cdot \mathrm{H}\left(\frac{\alpha x - \alpha y}{n - \alpha y}\right) - y \cdot \mathrm{H}\left(\frac{x-y}{y}\right) + y \cdot \mathrm{H}\left(\frac{x-y}{n-y}\right) \\
&\quad + n \cdot \mathrm{H}\left(\frac{y}{n}\right) - n \cdot \mathrm{H}\left(\frac{\alpha y}{n}\right) + n \cdot \mathrm{H}\left(\frac{\alpha x - \alpha y}{n - \alpha y}\right) - n \cdot \mathrm{H}\left(\frac{x-y}{n-y}\right). && (4.41)
\end{aligned}$$

From (4.39) to (4.40) we expand brackets and simplify, while from (4.40) to (4.41) we rearrange the terms for easy comparison.

Again $n > x > y$ ensures that the arguments of $\mathrm{H}(\cdot)$ are strictly less than half and $\mathrm{H}(p)$ increases monotonically with $p$. In (4.41) the difference of the first two terms in the first row is positive while the difference of the second two terms is negative. However, the whole sum of the first four terms is negative but very close to zero when $\alpha$ is close to one which is the regime that we will be considering. The difference of the last two terms in the second row is positive while the difference of the terms on bottom row is negative but due to the concavity and steepness of the Shannon entropy function the first positive difference is larger hence the sum of last four terms is positive. Since we can write $n = cy$ with $c > 1$ being an arbitrarily constant, then the positive sum in the second four terms dominates the negative sum in the first four terms. This gives the required results and hence concludes this proof and the proof of Lemma 4.3.6. $\square$

**Lemma 4.3.7.** *Given $\psi_n(\cdot)$ as defined in* (4.35) *then the following bound holds.*

$$\begin{aligned}\sum_{j=0}^{\lceil \log_2(s)\rceil-2} \left[q_j \cdot \psi_n\left(a_{Q_j}, a_{\left\lceil \frac{Q_j}{2}\right\rceil}, a_{\left\lfloor \frac{Q_j}{2}\right\rfloor}\right) + r_j \cdot \psi_n\left(a_{R_j}, a_{\left\lceil \frac{R_j}{2}\right\rceil}, a_{\left\lfloor \frac{R_j}{2}\right\rfloor}\right)\right] \\ + q_{\lceil \log_2(s)\rceil-1} \cdot \psi_n\left(a_2, d, d\right) \leq \sum_{j=0}^{\lceil \log_2(s)\rceil-1} 2^j \cdot \psi_n\left(a_{Q_j}, a_{\left\lfloor \frac{R_j}{2}\right\rfloor}, a_{\left\lfloor \frac{R_j}{2}\right\rfloor}\right), \qquad (4.42)\end{aligned}$$

*where* $a_{\frac{R_{\lceil \log_2(s)\rceil-1}}{2}} = d$.

*Proof.* The quantity in front of the summation in the top row of (4.42) can be bounded above in the following way.

$$\begin{aligned}
& q_j \cdot \psi_n\left(a_{Q_j}, a_{\left\lceil \frac{Q_j}{2}\right\rceil}, a_{\left\lfloor \frac{Q_j}{2}\right\rfloor}\right) + r_j \cdot \psi_n\left(a_{R_j}, a_{\left\lceil \frac{R_j}{2}\right\rceil}, a_{\left\lfloor \frac{R_j}{2}\right\rfloor}\right) && (4.43)\\
&= \left(s - 2^j\left\lceil \frac{s}{2^j}\right\rceil + 2^j\right) \cdot \psi_n\left(a_{Q_j}, a_{\left\lceil \frac{Q_j}{2}\right\rceil}, a_{\left\lfloor \frac{Q_j}{2}\right\rfloor}\right) \\
&+ \left(2^j\left\lceil \frac{s}{2^j}\right\rceil - s\right) \cdot \psi_n\left(a_{R_j}, a_{\left\lceil \frac{R_j}{2}\right\rceil}, a_{\left\lfloor \frac{R_j}{2}\right\rfloor}\right) && (4.44)\\
&< \left(s - 2^j\left\lceil \frac{s}{2^j}\right\rceil + 2^j\right) \cdot \psi_n\left(a_{Q_j}, a_{\left\lfloor \frac{Q_j}{2}\right\rfloor}, a_{\left\lfloor \frac{Q_j}{2}\right\rfloor}\right) \\
&+ \left(2^j\left\lceil \frac{s}{2^j}\right\rceil - s\right) \cdot \psi_n\left(a_{R_j}, a_{\left\lfloor \frac{R_j}{2}\right\rfloor}, a_{\left\lfloor \frac{R_j}{2}\right\rfloor}\right). && (4.45)\\
&< \left(s - 2^j\left\lceil \frac{s}{2^j}\right\rceil + 2^j\right) \cdot \psi_n\left(a_{Q_j}, a_{\left\lfloor \frac{R_j}{2}\right\rfloor}, a_{\left\lfloor \frac{R_j}{2}\right\rfloor}\right) \\
&+ \left(2^j\left\lceil \frac{s}{2^j}\right\rceil - s\right) \cdot \psi_n\left(a_{R_j}, a_{\left\lfloor \frac{R_j}{2}\right\rfloor}, a_{\left\lfloor \frac{R_j}{2}\right\rfloor}\right). && (4.46)\\
&< \left(s - 2^j\left\lceil \frac{s}{2^j}\right\rceil + 2^j\right) \cdot \psi_n\left(a_{Q_j}, a_{\left\lfloor \frac{R_j}{2}\right\rfloor}, a_{\left\lfloor \frac{R_j}{2}\right\rfloor}\right) \\
&+ \left(2^j\left\lceil \frac{s}{2^j}\right\rceil - s\right) \cdot \psi_n\left(a_{Q_j}, a_{\left\lfloor \frac{R_j}{2}\right\rfloor}, a_{\left\lfloor \frac{R_j}{2}\right\rfloor}\right). && (4.47)\\
&= 2^j \cdot \psi_n\left(a_{Q_j}, a_{\left\lfloor \frac{R_j}{2}\right\rfloor}, a_{\left\lfloor \frac{R_j}{2}\right\rfloor}\right). && (4.48)
\end{aligned}$$

From (4.44) to (4.45) we upper bound $\psi_n\left(a_{Q_j}, a_{\left\lceil \frac{Q_j}{2}\right\rceil}, a_{\left\lfloor \frac{Q_j}{2}\right\rfloor}\right)$ by $\psi_n\left(a_{Q_j}, a_{\left\lfloor \frac{Q_j}{2}\right\rfloor}, a_{\left\lfloor \frac{Q_j}{2}\right\rfloor}\right)$

and $\psi_n\left(a_{R_j}, a_{\left\lceil \frac{R_j}{2}\right\rceil}, a_{\left\lfloor \frac{R_j}{2}\right\rfloor}\right)$ by $\psi_n\left(a_{R_j}, a_{\left\lfloor \frac{R_j}{2}\right\rfloor}, a_{\left\lfloor \frac{R_j}{2}\right\rfloor}\right)$ using (4.36) of Lemma 4.3.6. We then upper bound $\psi_n\left(a_{Q_j}, a_{\left\lfloor \frac{Q_j}{2}\right\rfloor}, a_{\left\lfloor \frac{Q_j}{2}\right\rfloor}\right)$ by $\psi_n\left(a_{Q_j}, a_{\left\lfloor \frac{R_j}{2}\right\rfloor}, a_{\left\lfloor \frac{R_j}{2}\right\rfloor}\right)$, from (4.45) to (4.46), again using (4.36) of Lemma 4.3.6. From (4.46) to (4.47), using (4.37) of Lemma 4.3.6, we bound $\psi_n\left(a_{R_j}, a_{\left\lfloor \frac{R_j}{2}\right\rfloor}, a_{\left\lfloor \frac{R_j}{2}\right\rfloor}\right)$ by $\psi_n\left(a_{Q_j}, a_{\left\lfloor \frac{R_j}{2}\right\rfloor}, a_{\left\lfloor \frac{R_j}{2}\right\rfloor}\right)$. For the final step from (4.47) to (4.48) we factor out $\psi_n\left(a_{Q_j}, a_{\left\lfloor \frac{R_j}{2}\right\rfloor}, a_{\left\lfloor \frac{R_j}{2}\right\rfloor}\right)$ and then simplify.

Using $q_{\lceil \log_2(s)\rceil-1} + r_{\lceil \log_2(s)\rceil-1} = 2^{\lceil \log_2(s)\rceil-1}$ we bound $q_{\lceil \log_2(s)\rceil-1}$ by $2^{\lceil \log_2(s)\rceil-1}$. Then we add this to the summation of (4.48) for $j = 0, \ldots, \lceil \log_2(s)\rceil - 2$ establishing the bound of Lemma 4.3.7. □

Now we state and prove a lemma about the quantities $a_i$. During the proof we will make a statement about the $a_i$ using their expected values $\hat{a}_i$ which follows from a maximum likelihood analogy.

**Lemma 4.3.8.** *The problem*

$$\max_{a_s,\ldots,a_2} \sum_{i=1}^{\lceil s/2\rceil} \frac{s}{2i} \cdot \psi_n\left(a_{2i}, a_i, a_i\right) \tag{4.49}$$

*has a global maximum and the maximum occurs at the expected values of the $a_i$, $\hat{a}_i$ given by*

$$\hat{a}_{2i} = \hat{a}_i\left(2 - \frac{\hat{a}_i}{n}\right) \quad \text{for} \quad i = 1, 2, 4, \ldots, \lceil s/2\rceil, \tag{4.50}$$

*which are a solution of the following polynomial system.*

$$\begin{aligned} a_{\lceil s/2\rceil}^2 - 2na_{\lceil s/2\rceil} + na_s &= 0, \\ a_{2i}^3 - 2a_ia_{2i}^2 + 2a_i^2a_{2i} - a_i^2a_{4i} &= 0 \\ &\text{for} \quad i = 1, 2, \ldots, \lceil s/4\rceil. \end{aligned} \tag{4.51}$$

*where $a_1 = d$. If $a_s$ is constrained to be less than $\hat{a}_s$, then there is a different global maximum, instead the $a_i$ satisfy the following system*

$$\begin{aligned} a_{2i}^3 - 2a_ia_{2i}^2 + 2a_i^2a_{2i} - a_i^2a_{4i} &= 0 \\ &\text{for} \quad i = 1, 2, 4, \ldots, \lceil s/4\rceil, \end{aligned} \tag{4.52}$$

*again with $a_1 = d$.*

*Proof.* Define

$$\widetilde{\Psi}_n\left(a_s, \ldots, a_2, d\right) := \sum_{i=1}^{\lceil s/2\rceil} \frac{s}{2i} \cdot \psi_n\left(a_{2i}, a_i, a_i\right). \tag{4.53}$$

Using the definition of $\psi_n(\cdot)$ in (4.35) we therefore have $\widetilde{\Psi}_n\left(a_s,\dots,a_2,d\right)$ equal to the following.

$$\sum_{i=1}^{\lceil s/2\rceil}\frac{s}{2i}\cdot\left[a_i\cdot\mathrm{H}\left(\frac{a_{2i}-a_i}{a_i}\right)+(n-a_i)\cdot\mathrm{H}\left(\frac{a_{2i}-a_i}{n-a_i}\right)-n\cdot\mathrm{H}\left(\frac{a_i}{n}\right)\right]. \tag{4.54}$$

The gradient of $\widetilde{\Psi}_n\left(a_s,\dots,a_2,d\right)$, $\nabla\widetilde{\Psi}_n\left(a_s,\dots,a_2,d\right)$ is given by

$$\left(\log\left[\frac{\left(2a_{\lceil s/2\rceil}-a_s\right)(n-a_s)}{\left(a_s-a_{\lceil s/2\rceil}\right)^2}\right],\frac{s}{2i}\cdot\log\left[\frac{a_{2i}\left(a_{4i}-a_{2i}\right)\left(2a_i-a_{2i}\right)}{\left(2a_{2i}-a_{4i}\right)\left(a_{2i}-a_i\right)^2}\right]\right)^T,$$
$$\text{for}\quad i=1,2,4,\dots,\lceil s/4\rceil, \tag{4.55}$$

where $v^T$ is the transpose of the vector $v$. Obtaining the critical points at $\nabla\widetilde{\Psi}_n\left(a_s,\dots,d\right)=0$ leads to the polynomial system (4.51).

The Hessian, $\nabla^2\widetilde{\Psi}_n\left(a_s,\dots,a_2,d\right)$ at these optimal $a_i$ which are the solutions to the polynomial system (4.51) is negative definite which implies that this unique critical point is a global maximum point. Let the solution of the system be the $\hat{a}_i$ then they satisfy a recurrence formula (4.50) which is equivalent to their expected values as explained in the paragraph that follows.

We estimate the uniformly distributed parameter relating $a_{2i}$ to $a_i$. The best estimator of this parameter is the maximum likelihood estimator which we calculate from the maximum log-likelihood estimator (MLE). The summation of the $\psi_n(\cdot)$ is the logarithm of the join density functions for the parameter relating the $a_i$. The MLE is obtained by maximizing this summation and it corresponds to the expected log-likelihood. Therefore, the parameters given implicitly by (4.50) are the expected log-likelihood which implies that the values of the $\hat{a}_j$ in (4.50) are the expected values of the $a_i$.

If we restrict $a_s$ to take a fixed value, then $\nabla\widetilde{\Psi}_n\left(a_s,\dots,a_2,d\right)$ is given by

$$\left(\frac{s}{2i}\cdot\log\left[\frac{a_{2i}\left(a_{4i}-a_{2i}\right)\left(2a_i-a_{2i}\right)}{\left(2a_{2i}-a_{4i}\right)\left(a_{2i}-a_i\right)^2}\right]\right)^T\quad\text{for}\quad i=1,2,4,\dots,\lceil s/4\rceil. \tag{4.56}$$

Obtaining the critical points by solving $\nabla\widetilde{\Psi}_n\left(a_s,\dots,a_2,d\right)=0$ leads to the polynomial system (4.52).

Given $a_s$, the Hessian, $\nabla^2\widetilde{\Psi}_n\left(a_s,\dots,a_2,d\right)$ at these optimal $a_i$ which are the solutions to the polynomial system (4.52) is negative definite which implies that this unique critical point is a global maxima; this case differs from a maximum likelihood estimation because of the extra constraint of fixing $a_s$. □

The dyadic splitting technique we employ requires greater care of the polynomial term in the large deviation bound of $\mathrm{P}_n\left(x,y,z\right)$ in (4.14); Lemma 4.3.10 establishes the polynomial term.

**Definition 4.3.9.** *$P_n(x,y,z)$ defined in (4.14) satisfies the upper bound*

$$P_n(x,y,z) \leq \pi(x,y,z)\exp(\psi_n(x,y,z)) \tag{4.57}$$

*with bounds of $\pi(x,y,z)$ given in Lemma 4.3.10.*

**Lemma 4.3.10.** *From the definition of $\pi(x,y,z)$ and $P_n(x,y,z)$ in (4.57) and (4.14) respectively, $\pi(x,y,z)$ has the following cases.*

$$\left(\frac{5}{4}\right)^4\left[\frac{yz(n-y)(n-z)}{2\pi n(y+z-x)(x-y)(x-z)(n-x)}\right]^{\frac{1}{2}} \quad \textit{if} \quad \{y,z\}<x<y+z \tag{4.58}$$

$$\left(\frac{5}{4}\right)^3\left[\frac{y(n-z)}{n(y-z)}\right]^{\frac{1}{2}} \quad \textit{if} \quad x=y>z; \tag{4.59}$$

$$\left(\frac{5}{4}\right)^3\left[\frac{(n-y)(n-z)}{n(n-y-z)}\right]^{\frac{1}{2}} \quad \textit{if} \quad x=y+z; \tag{4.60}$$

$$\left(\frac{5}{4}\right)^2\left[\frac{2\pi z(n-z)}{n}\right]^{\frac{1}{2}} \quad \textit{if} \quad x=y=z. \tag{4.61}$$

*Proof.* From Definition 4.3.9 the quantity $\pi(x,y,z)$ is the polynomial portion of the large deviation upper bound. Within this proof we express this by

$$\pi(x,y,z) = poly\left[\binom{y}{y+z-x}\binom{n-y}{x-y}\binom{n}{z}^{-1}\right]. \tag{4.62}$$

We derive the upper bound $\pi(x,y,z)$ using the Stirling's inequality. The right inequality of (2.11) is used to upper bound $\binom{y}{y+z-x}$ and $\binom{n-y}{x-y}$ and the left inequality of (2.11) is used to lower bound $\binom{n}{z}$. If $\{y,z\}<x<y+z$ the bound is well defined and simplifies to (4.58).

If $x=y>z$ (4.58) is undefined; however, substituting $y$ for $x$ in (4.62) gives $\binom{y}{y+z-x}=\binom{y}{z}$ and $\binom{n-y}{x-y}=\binom{n-y}{0}=1$. We upper bound the product $\binom{y}{z}\binom{n}{z}^{-1}$ using the right inequality in (2.11) to bound $\binom{y}{z}$ from above and the left inequality in (2.11) to bound from below $\binom{n}{z}$. The resulting polynomial part of the product simplifies to (4.59).

If $x=y+z$, then $\binom{y}{y+z-x}=\binom{y}{0}=1$ and $\binom{n-y}{x-y}=\binom{n-y}{z}$. As above, we upper bound the product of $\binom{n-y}{x-y}$ and $\binom{n}{z}^{-1}$ using (2.11) and simplify the polynomial part of this product to get (4.60). If instead $x=y=z$, then $\binom{y}{y+z-x}=\binom{y}{0}$ and $\binom{n-y}{x-y}=\binom{n-y}{0}$ both of which equal 1. Therefore the bound only involves $\binom{n}{z}^{-1}$ which we bound using (2.11) and the resulting polynomial part simplifies to (4.61). □

**Corollary 4.3.11.** *If $n>2y$, then $\pi(y,y,y)$ is monotonically increasing in $y$.*

*Proof.* If $n>2y$, (4.61) implies that $\pi(y,y,y)$ is proportional to $\sqrt{y}$, i.e. $\pi(y,y,y)=c\sqrt{y}$, with $c>0$ and $c\sqrt{y}$ is monotonic in $y$. □

## 4.4 Implications for Compressed Sensing Algorithms

Here we revisit the use of restricted isometry constants to analyse compressed sensing algorithms. In Section 4.4.1 we discuss theoretical guarantees of performance of algorithms based on both RIC$_1$ and RIC$_2$. In Section 4.4.2 we present quantitative comparison of performance guarantees of some of these algorithms proposed for the kind of matrices we consider in Definition 4.2.1 and we also feature a comparison of $\ell_1$-minimization for dense Gaussian matrices to that of the sparse matrices we consider here.

### 4.4.1 Performance Guarantees of Compressed Sensing Algorithms

As shown in Section 2.5, RIC$_2$ bounds were used to derive sampling theorems for compressed sensing algorithms – $\ell_1$-minimization and the greedy algorithms for dense matrices, IHT, CoSAMP, and SP. Furthermore, using the phase transition framework with RIC$_2$ bounds Blanchard et. al. compared performance of these algorithms in [20]. In a similar vein, as another key contribution of this work we provide sampling theorems for $\ell_1$-minimization and combinatorial greedy algorithms, EMP, SMP, SSMP, LDDSR and ER, proposed for SE and SSE matrices.

Theoretical guarantees have been given for $\ell_1$ recovery and recovery by other greedy algorithms including EMP, SMP, SSMP, LDDSR and ER designed to do compressed sensing recovery with adjacency matrices of lossless expander graphs and by extension SSE matrices. Sparse matrices have been observed to have recovery properties comparable to dense matrices for $\ell_1$-minimization and some of the aforesaid algorithms, see [15, 16, 79, 149, 148] and the references therein. Based on theoretical guarantees, we derived sampling theorems and present here phase transition curves which are plots of phase transition functions $\rho^{alg}(\delta; d, \epsilon)$ of algorithms such that for $k/n \rightarrow \rho < (1-\gamma)\rho^{alg}(\delta; d, \epsilon),\ \gamma > 0$, a given algorithm is guaranteed to recovery all $k$-sparse signals with overwhelming probability on the draw of the sensing matrix $A$. This probability approaches 1 exponentially in $n$.

#### $\ell_1$-minimization

Berinde et. al. showed in [15] that $\ell_1$-minimization can be used to perform signal recovery with binary matrices coming from expander graphs. We reproduce the formal statement of this guarantee in the following theorem, the proof of which can be found in [15, 16].

**Theorem 4.4.1** (Theorem 3, [15], Theorem 1, [16])**.** *Let $A$ be an adjacency matrix of a lossless $(k, d, \epsilon)$-expander graph with $\alpha(\epsilon) = 2\epsilon/(1-2\epsilon) < 1/2$. Given any two vectors $x$, $\hat{x}$ such that $Ax = A\hat{x}$, and $||\hat{x}||_1 \leq ||x||_1$, let $x_k$ be the largest (in magnitude) coefficients of $x$, then*

$$||x - \hat{x}||_1 \leq \frac{2}{1 - 2\alpha(\epsilon)} ||x - x_k||_1. \tag{4.63}$$

The condition that $\alpha(\epsilon) = 2\epsilon/(1-2\epsilon) < 1/2$ implies the sampling theorem stated as Corollary 4.4.2, that when satisfied ensures a positive upper bound in (4.63). The resulting sampling theorem is given by $\rho^{\ell_1}(\delta; d, \epsilon)$ using $\epsilon = 1/6$ from Corollary 4.4.2.

**Corollary 4.4.2** ([15]). *$\ell_1$-minimization is guaranteed to recover any $k$-sparse vector from its linear measurement by an adjacency matrix of a lossless $(k, d, \epsilon)$-expander graph with $\epsilon < 1/6$.*

*Proof.* Setting the denominator of the fraction in the right hand side of (4.63) to be greater than zero gives the required result. □

### Sequential Sparse Matching Pursuit (SSMP)

Introduced by Indyk and Ruzic in [17], SSMP has evolved as an improvement of Sparse Matching Pursuit (SMP) which was an improvement on Expander Matching Pursuit (EMP). EMP also introduced by Indyk and Ruzic in [78] uses a voting-like mechanism to identify and eliminate large (in magnitude) components of the signal. EMP's drawback is that the *empirical* number of measurements it requires to achieve correct recovery is suboptimal. SMP, introduced by Berinde, Indyk and Ruzic in [18], improved on the drawback of EMP. However, its original version had convergence problems when the input parameters ($k$ and $n$) fall outside the theoretically guaranteed region. This is fixed in the SMP package which forces convergence when the user provides an additional convergence parameter. In order to correct the aforementioned problems of EMP and SMP, Indyk and Ruzic developed SSMP. It is a version of SMP where updates are done sequentially instead of in parallel, consequently convergence is automatically achieved. All three algorithms have the same theoretical recovery guarantees, which we state in Theorem 4.4.3, but SSMP has better empirical performances compared to its predecessors.

```
Input: $A$, $y$, $\eta$
Output: $k$-sparse approximation $\hat{x}$ of the target signal $x$
Initialization:
  1. Set $j = 0$
  2. Set $x_j = 0$
Iteration: Repeat $T = \mathcal{O}\left(\log\left(\|x\|_1/\eta\right)\right)$ times
  1. Set $j = j + 1$
  2. Repeat $(c-1)k$ times
     a) Find a coordinate $i$ and an increment $z$ that minimizes $\|A\left(x_j + ze_i\right) - y\|_1$
     b) Set $x_j$ to $x_j + ze_i$
  3. Set $x_j = H_k\left(x_j\right)$
Return $\hat{x} = x^T$
```

Table 4.1: **Algorithm 5** – Sequential Sparse Matching Pursuit (SSMP) [17].

Algorithm 5 in Table 4.1 is a pseudo-code of the SSMP algorithm based on the following problem setting. The measurement matrix $A$ is an $n \times N$ adjacency matrix of a lossless $((c+1)k, d, \epsilon/2)$-expander scaled by $d$ and $A$ has a lower RIC$_1$, $L\left((c+1)k, n, N\right) = \epsilon$. The measurement vector $y = Ax + e$ where $e$ is a noise vector and $\eta = \|e\|_1$. We denote the hard thresholding operator by $H_k(z)$, it sets to zero all but the largest, in magnitude, $k$ entries of $z$.

The recovery guarantees for SSMP (also for EMP and SMP) are formalized by the following theorem from which we deduce the recovery condition (sampling theorem) in terms of $\epsilon$ in Corollary 4.4.4.

**Theorem 4.4.3** (Theorem 10, [78]). *Let $A$ be an adjacency matrix of a lossless $(k,d,\epsilon)$-expander graph with $\epsilon < 1/16$. Given a vector $y = Ax + e$, SSMP (also EMP and SMP) returns approximation vector $\hat{x}$ satisfying*

$$||x - \hat{x}||_1 \leq \frac{1-4\epsilon}{1-16\epsilon}||x - x_k||_1 + \frac{6}{(1-16\epsilon)d}||e||_1, \tag{4.64}$$

*where $x_k$ is the $k$ largest (in magnitude) coordinates of $x$.*

**Corollary 4.4.4** ([78]). *SSMP, EMP, and SMP are all guaranteed to recover any $k$-sparse vector from its linear measurement by an adjacency matrix of a lossless $(k,d,\epsilon)$-expander graph with $\epsilon < 1/16$.*

### Expander Recovery (ER)

Introduced by Jafarpour et. al. in [79, 80], ER is an improvement on an earlier algorithm introduced by Xu and Hassibi in [148] known as Left Degree Dependent Signal Recovery (LDDSR). The improvement was mainly on the number of iterations used by the algorithms and the type of expanders used, from $(k,d,1/4)$-expanders for LDDSR to $(k,d,\epsilon)$-expander for any $\epsilon < 1/4$ for ER. Both algorithms use this concept of a *gap* defined below.

**Definition 4.4.5** (gap, [148, 79, 80]). *Let $x$ be the original signal and $y = Ax$. Furthermore, let $\hat{x}$ be our estimate for $x$. For each value $y_i$ we define a gap $g_i$ as:*

$$g_i = y_i - \sum_{j=1}^{N} A_{ij}\hat{x}_j. \tag{4.65}$$

Algorithm 6 of Table 4.2 is a pseudo-code of the ER algorithm for an original $k$-sparse signal $x \in \mathbb{R}^N$ and the measurements $y = Ax$ with an $n \times N$ measurement matrix $A$ that is an adjacency matrix of a lossless $(2k,d,\epsilon)$-expander and $\epsilon < 1/4$. The measurements are assumed to be without noise, so we aim for exact recovery. The authors of [79, 80] have a modified version of the algorithm for when $x$ is almost $k$-sparse.

We state Theorem 4.4.6 which give recovery guarantees for ER. Directly from this theorem we read-off the recovery condition in terms of $\epsilon$ for Corollary 4.4.7 which needs no further proof.

**Theorem 4.4.6** (Theorem 6, [80]). *Let $A \in \mathbb{R}^{n\times N}$ be the adjacency matrix of a lossless $(2k,d,\epsilon)$-expander graph, where $\epsilon \leq 1/4$ and $n = \mathcal{O}(k\log(N/k))$. Then, for any $k$-sparse signal $x$, given $y = Ax$, ER recovers $x$ successfully in at most $2k$ iterations.*

```
Input: $A$, $y$
Output: $k$-sparse approximation $\hat{x}$ of the original signal $x$
Initialization:
  1. Set $\hat{x} = 0$
Iteration: Repeat at most $2k$ times
  1. if $y = A\hat{x}$ then
  2.     return $\hat{x}$ and exit
  3. else
  4.     Find a variable node $\hat{x}_j$ such that at least $(1 - 2\epsilon)d$ of the measurements it
          participated in, have identical gap $g_i$
  5.     Set $\hat{x}_j = \hat{x}_j + g_i$, and go to 2.
  6. end if
```

Table 4.2: **Algorithm 6** – Expander Recovery (ER) [79, 80].

**Corollary 4.4.7.** *ER is guaranteed to recovery $x$ if $\epsilon \leq 1/4$.*

### 4.4.2 Quantitative Comparisons of Compressed Sensing Algorithms

Using the phase transition framework with the theoretical performance guarantees given above we make a quantitative comparison of the greedy algorithms discussed above. We used RIC$_2$ based analysis of $\ell_1$-minimization for Gaussian matrices in [19, 20] and the RIC$_1$ based analysis of $\ell_1$-minimization discussed above to also make a quantitative comparison of $\ell_1$-minimization for the dense versus sparse matrices.

To derive the phase transition functions, $\rho^{alg}(\delta; d, \epsilon)$, for the associated algorithm in the RIC$_1$ case we replace $\rho^{exp}(\delta; d, \epsilon)$ by $\rho^{alg}(\delta; d, \epsilon)$ in Corollary 4.2.8 and we use the $\epsilon$ value from the recovery conditions given in the preceding section to compute $\rho^{alg}(\delta; d, \epsilon)$. Precisely, Corollary 4.4.2 gave the $\epsilon$ value used to derive $\rho^{\ell_1}(\delta; d, \epsilon)$ for $\ell_1$-minimization; Corollary 4.4.4 gave the $\epsilon$ value used to derive $\rho^{SSMP}(\delta; d, \epsilon)$ for SSMP; and Corollary 4.4.7 gave the $\epsilon$ value used to derive $\rho^{ER}(\delta; d, \epsilon)$ for ER.

The left panel of Figure 4.5 compares the phase transition plot of $\rho^{SSMP}(\delta; d, \epsilon)$ for SSMP (also for EMP and SMP), the phase transition of plot $\rho^{ER}(\delta; d, \epsilon)$ for ER (also of LDDSR) and the phase transition plot of $\rho^{\ell_1}(\delta; d, \epsilon)$ for $\ell_1$-minimization. Remarkably, for ER and LDDSR recovery is guaranteed for a larger portion of the $(\delta, \rho)$ plane than is guaranteed by the theory for $\ell_1$-minimization using sparse matrices; however, $\ell_1$-minimization has a larger recovery region than does SSMP, EMP, and SMP. In has been shown in [17] that SSMP and SMP have similar average numerical behaviour to $\ell_1$-minimization for SE matrices.

The right panel of Figure 4.5 shows a comparison of the phase transition of $\ell_1$-minimization as presented by Blanchard et. al. in [20] for dense Gaussian matrices based on RIC$_2$ analysis and the phase transition we derived here for the sparse binary matrices coming from lossless expander based on RIC$_1$ analysis. This shows a remarkable difference between the two with sparse matrices having better performance guarantees; this improvement is achieved through

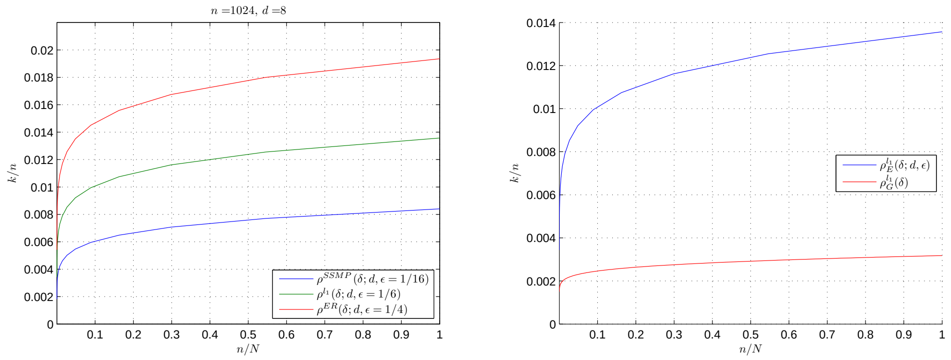

Figure 4.5: *Left panel:* Phase transition curves $\rho^{alg}(\delta; d, \epsilon)$ computed over finite values of $\delta \in (0, 1)$ with $d$ fixed and the different $\epsilon$ values for each algorithm - 1/4, 1/6 and 1/16 for ER, $\ell_1$ and SSMP respectively. *Right panel:* Phase transition plots of $\ell_1$; $\rho^{\ell_1}(\delta)$ for Gaussian matrices and $\rho^{\ell_1}(\delta; d, \epsilon)$ for adjacency matrices of expander graphs.

RIC$_1$ being more closely related to $\ell_1$-minimization than is RIC$_2$. However, $\ell_1$-minimization average numerical performance (weak phase transition) for SE matrices has been shown to be the same in [15].

Note that the phase transition curves for the sparse matrices (SE and SSE) are computed for finite $(k, n, N, d, \epsilon)$ unlike that for the dense Gaussian case. This is because the derivation of $\rho^{alg}(\delta; d, \epsilon)$ involves $\Psi(k, d, \epsilon)$ in (4.11) which is defined in terms of $\Psi(a_s, \ldots, a_2, d)$ in (4.3). Precisely, the asymptotic approximation of $\rho^{alg}(\delta; d, \epsilon)$ would require a closed form solution to the polynomial equation (4.5). This implicit dependence of $\rho^{alg}(\delta; d, \epsilon)$ on $k, n, N, d$ and $\epsilon$ through $\Psi(k, d, \epsilon)$ made it difficult to deduce the asymptotic behaviour of $\rho^{alg}(\delta; d, \epsilon)$. Hence we numerically compute $\rho^{alg}(\delta; d, \epsilon)$ for every instance of $(k, n, N, d, \epsilon)$ we plotted.

## 4.5 Proofs

Here we present the proof of theorems and corollaries from Section 4.2 and Section 4.3.1. We begin with the proof of Theorem 4.2.4 by first showing that it holds for small sizes examples in Section 4.5.1 and give the proof for large $s$ in Section 4.5.2.

### 4.5.1 Theorem 4.2.4 - Examples of Small Problems

We will present three examples of small size problems with $s = 2$, $s = 3$ and $s = 8$. In addition to being base cases that show that Theorem 4.2.4 holds, these examples for small $s$ are insightful, making it easy for the reader to follow the more complicated proof of the theorem for large $s$. These examples could also be used to confirm statements (lemmas, corollaries and propositions) made in the proof for large $s$.

**Example 1:** For $s = 2$ we have $A_2 = A_1^1 \cup A_1^2$ where $A_1^1$ and $A_1^2$ are composed of one column each. Therefore

$$\begin{aligned}
\operatorname{Prob}\left(|A_2| \leq a_2\right) &= \operatorname{Prob}\left(\left|A_1^1 \cup A_1^2\right| \leq a_2\right) && (4.66)\\
&= \sum_{l_2=d}^{a_2} \operatorname{Prob}\left(\left|A_1^1 \cup A_1^2\right| = l_2\right), && (4.67)\\
&= \sum_{l_2=d}^{a_2} \mathrm{P}_n\left(l_2, d, d\right) \cdot \prod_{j=1}^{2} \operatorname{Prob}\left(\left|A_1^j\right| = d\right), && (4.68)\\
&= \sum_{l_2=d}^{a_2} \mathrm{P}_n\left(l_2, d, d\right). && (4.69)
\end{aligned}$$

From (4.66) to (4.67) we sum over all possible events. Note that $l_2$ cannot be less than $d$ since for $j = 1, 2$, $\left|A_1^j\right| = d$. Now given $\left|A_1^j\right|$ for $j = 1, 2$ the probability in (4.67) becomes the probability of the size of the intersection multiplied by the probabilities of $\left|A_1^j\right|$, thus (4.68). Each column has $d$ ones, therefore $\operatorname{Prob}\left(\left|A_1^1\right| = d\right) = 1$ and $\operatorname{Prob}\left(\left|A_1^2\right| = d\right) = 1$, hence (4.69).

Using the definition of $\mathrm{P}_n(\cdot)$ in Lemma 4.3.3 and the Stirling's formula (2.11) we can bound (4.69) as thus.

$$\sum_{l_2=d}^{a_2} \mathrm{P}_n\left(l_2, d, d\right) < \sum_{l_2=d}^{2d} \pi\left(l_2, d, d\right) \cdot e^{\psi_n(l_2,d,d)}, \tag{4.70}$$

where $\pi(\cdot)$ is a polynomial term resulting from the upper bound of $\mathrm{P}_n(\cdot)$ using Stirling's formula. We also bound the upper limit of the sum using the fact that $a_2 \leq 2d$.

Now let $l_2 = a_2$ maximize the exponential term in (4.70) then we pull the exponential term out of the sum to get the following bound.

$$\begin{aligned}
\sum_{l_2=d}^{2d} \pi\left(l_2, d, d\right) \cdot e^{\psi_n(l_2,d,d)} &< e^{\psi_n(a_2,d,d)} \cdot \sum_{l_2=d}^{2d} \pi\left(l_2, d, d\right) && (4.71)\\
&< d \cdot \pi\left(d, d, d\right) \cdot e^{\psi_n(a_2,d,d)} && (4.72)\\
&= d \cdot \left(\frac{5}{4}\right)^2 \cdot \sqrt{\frac{2\pi d(n-d)}{n}} \cdot e^{\psi_n(a_2,d,d)} && (4.73)\\
&< \left(\frac{5}{4}\right)^2 \cdot \sqrt{2\pi d^3} \cdot e^{\psi_n(a_2,d,d)}. && (4.74)
\end{aligned}$$

From (4.71) to (4.72) we use the fact that $\pi(x, y, z)$ is greatest when $x = y = z$ and we bound the summation in (4.71) with the product of this maximum value of $\pi(d, d, d)$ and the number of terms in the sum. From (4.72) to (4.73) we use (4.61) to evaluate $\pi(d, d, d)$ and we upper bound (4.73) by (4.74) by forgoing the subtraction of $d/n$ under the square root.

Then we manipulate the factor multiplying the exponential in (4.74) in order to get it in the format of the bound of (4.1). So we multiply (4.74) by $\frac{2}{25\sqrt{2\pi(2^3)d^3}}$ and its reciprocal to get

$$\frac{2}{25\sqrt{2\pi\left(2^3\right)d^3}} \cdot \frac{25\sqrt{2\pi\left(2^3\right)d^3}}{2} \cdot \frac{25}{16} \cdot \sqrt{2\pi d^3} \cdot e^{\psi_n(a_2,d,d)} \tag{4.75}$$

$$= \frac{2}{25\sqrt{2\pi\left(2^3\right)d^3}} \cdot \frac{25}{2} \cdot \frac{25}{16} \cdot 4\sqrt{2\pi}d^3 \cdot e^{\psi_n(a_2,d,d)} \tag{4.76}$$

$$= \frac{2}{25\sqrt{2\pi\left(2^3\right)d^3}} \cdot 5^4 \cdot \frac{\sqrt{2\pi}}{8} \cdot d^3 \cdot e^{\psi_n(a_2,d,d)} \tag{4.77}$$

$$< \frac{2}{25\sqrt{2\pi\left(2^3\right)d^3}} \cdot (5d)^6 \cdot e^{\psi_n(a_2,d,d)} \tag{4.78}$$

$$= \frac{2}{25\sqrt{2\pi\left(2^3\right)d^3}} \cdot \exp\left[6\log(5d) + \psi_n\left(a_2,d,d\right)\right]. \tag{4.79}$$

From (4.75) through to (4.77) we simplify and from (4.77) to (4.78) we upper bound $\frac{\sqrt{2\pi}}{8}$ by $d$, since $d \geq 1$, and upper bound $(5d)^4$ by $(5d)^6$. Then we rewrite $(5d)^6$ as $\exp\left[6\log(5d)\right]$ from (4.78) to (4.79). This is consistent with Theorem 4.2.4 with $p_{max}(s,d) = \frac{2}{25\sqrt{2\pi(2^3)d^3}}$ and $\Psi\left(a_2,d\right) = \frac{1}{n}\left[6\log(5d) + \psi_n\left(a_2,d,d\right)\right]$ for the case $s = 2$ .

**Example 2:** For $s = 3$ we have $|A_3| = \left|A_2^1 \cup A_1^2\right|$ where $A_1^2$ and $A_2^1$ are composed of one and two columns respectively. Therefore,

$$\text{Prob}\left(|A_3| \leq a_3\right) = \text{Prob}\left(\left|A_2^1 \cup A_1^2\right| \leq a_3\right) \tag{4.80}$$

$$= \sum_{l_3=\min\left(l_2^1,d\right)}^{\min\left(\min\left(2l_2^1,3d\right),a_3\right)} \sum_{l_2^1=d}^{\min(2d,l_3)} \text{Prob}\left(\left|A_2^1 \cup A_1^2\right| = l_3\right) \tag{4.81}$$

$$= \sum_{l_3}\sum_{l_2^1} \text{P}_n\left(l_3, l_2^1, d\right) \cdot \text{Prob}\left(\left|A_2^1\right| = l_2^1\right) \cdot \text{Prob}\left(\left|A_1^2\right| = d\right). \tag{4.82}$$

From (4.80) to (4.81) we sum over all possible events. From (4.81) to (4.82) we rewrite the probability as a product of the probability of the cardinalities of $\left|A_2^1\right|$ and $\left|A_1^2\right|$ and their intersection.

We use the fact that $\text{Prob}\left(\left|A_1^2\right| = d\right) = 1$ and we split $A_2^1$ into $A_1^3$ and $A_1^4$ to have (4.82) become

$$\sum_{l_3}\sum_{l_2^1} \text{P}_n\left(l_3, l_2^1, d\right) \cdot \text{Prob}\left(\left|A_1^3 \cup A_1^4\right| = l_2^1\right) \tag{4.83}$$

$$= \sum_{l_4}\sum_{l_2^1} \text{P}_n\left(l_3, l_2^1, d\right) \cdot \text{P}_n\left(l_2^1, d, d\right) \cdot \text{Prob}\left(\left|A_1^3\right| = d\right) \cdot \text{Prob}\left(\left|A_1^4\right| = d\right) \tag{4.84}$$

$$= \sum_{l_3}\sum_{l_2^1} \text{P}_n\left(l_3, l_2^1, d\right) \cdot \text{P}_n\left(l_2^1, d, d\right). \tag{4.85}$$

From (4.83) to (4.84) we rewrite $\text{Prob}\left(\left|A_1^2 \cup A_1^3\right| = l_2^1\right)$ as a product of the cardinality of the intersection and the probability of $\left|A_1^3\right|$ and $\left|A_1^4\right|$ while from (4.84) to (4.85) we use the fact that $\text{Prob}\left(\left|A_1^j\right| = d\right) = 1$ for $j = 3, 4$.

Again using the definition of $\mathrm{P}_n(\cdot)$ in Lemma 4.3.3 and the Stirling's approximation we can upper bound (4.85) by

$$\sum_{l_3=2d}^{3d} \sum_{l_2^1=d}^{2d} \pi\left(l_3, l_2^1, d\right) \cdot e^{\psi_n\left(l_3, l_2^1, d\right)} \cdot \pi\left(l_2^1, d, d\right) \cdot e^{\psi_n\left(l_2^1, d, d\right)} \tag{4.86}$$

$$< \exp\left[\psi_n\left(a_3, a_2, d\right) + \psi_n\left(a_2, d, d\right)\right] \cdot \sum_{l_3=2d}^{3d} \sum_{l_2^1=d}^{2d} \pi\left(l_3, l_2^1, d\right) \cdot \pi\left(l_2^1, d, d\right) \tag{4.87}$$

$$< d^2 \cdot \left[\pi\left(d, d, d\right)\right]^2 \cdot \exp\left[\psi_n\left(a_3, a_2, d\right) + \psi_n\left(a_2, d, d\right)\right]. \tag{4.88}$$

From (4.86) to (4.87) we maximize the exponential terms at $l_2^1 = a_2$ and $l_3 = a_3$ and pull it out of the summation. Then from (4.87) to (4.88) we use the maximum of $\pi(\cdot)$ given by (4.61) and multiply this by the number of the terms in the sums to upper bound the summations.

Now we evaluate $\pi(d, d, d)$ using (4.61) to have (4.88) become

$$d^2 \cdot \left[\left(\frac{5}{4}\right)^2 \cdot \sqrt{\frac{2\pi d(n-d)}{n}}\right]^2 \cdot \exp\left[\psi_n\left(a_3, a_2, d\right) + \psi_n\left(a_2, d, d\right)\right] \tag{4.89}$$

$$< \left(\frac{5}{4}\right)^4 \cdot 2\pi d^3 \cdot \exp\left[\psi_n\left(a_3, a_2, d\right) + \psi_n\left(a_2, d, d\right)\right] \tag{4.90}$$

$$= \frac{2}{25\sqrt{2\pi\left(3^3\right)d^3}} \cdot \frac{25\sqrt{2\pi\left(3^3\right)d^3}}{2} \left(\frac{5}{4}\right)^4 2\pi d^3 \cdot \exp\left[\psi_n\left(a_3, a_2, d\right) + \psi_n\left(a_2, d, d\right)\right] \tag{4.91}$$

$$< \frac{2}{25\sqrt{2\pi\left(3^3\right)d^3}} \cdot (5d)^9 \cdot \exp\left[\psi_n\left(a_3, a_2, d\right) + \psi_n\left(a_2, d, d\right)\right] \tag{4.92}$$

$$= \frac{2}{25\sqrt{2\pi\left(3^3\right)d^3}} \cdot \exp\left[9\log\left(5d\right) + \psi_n\left(a_3, a_2, d\right) + \psi_n\left(a_2, d, d\right)\right]. \tag{4.93}$$

From (4.89) to (4.90) we upper bound the term in the square root and from (4.90) to (4.91) we multiply the factor in front of the exponential by $\frac{2}{25\sqrt{2\pi(3^3)d^3}}$ and its reciprocal. From (4.91) to (4.92) we bound $\frac{25\sqrt{2\pi(3^3)d^3}}{2}\left(\frac{5}{4}\right)^4 2\pi d^3$ by $(5d)^9$ since $d \geq 1$; while from (4.92) to (4.93) we rewrite $(5d)^9$ as $\exp\left[9\log\left(5d\right)\right]$. Expression (4.93) is consistent with the bound in Theorem 4.2.4 with $p_{max}(s, d) = \frac{2}{25\sqrt{2\pi(3^3)d^3}}$ and $\Psi\left(a_3, a_2, d\right) = \frac{1}{n}\left[9\log\left(5d\right) + \psi_n\left(a_3, a_2, d\right) + \psi_n\left(a_2, d, d\right)\right]$ for the case $s = 3$.

**Example 3:** For $s = 8$ we have $|A_8| = \left|A_4^1 \cup A_4^2\right|$ where $A_4^2$ and $A_4^1$ are composed of four columns each respectively. Therefore,

$$\mathrm{Prob}\left(|A_8| \leq a_8\right) = \mathrm{Prob}\left(\left|\bigcup_{j=1}^{2} A_4^j\right| \leq a_8\right) \tag{4.94}$$

$$= \sum_{l_8=\min\left(l_4^1, l_4^2\right)}^{\min\left(2\min\left(l_4^1, l_4^2\right), a_8\right)} \sum_{\substack{l_4^j=\min\left(l_2^{2j-1}, l_2^{2j}\right) \\ j=1,2}}^{\min\left(2\min\left(l_2^{2j-1}, l_2^{2j}\right), l_8\right)} \mathrm{Prob}\left(\left|\bigcup_{j=1}^{2} A_4^j\right| = l_8\right) \tag{4.95}$$

$$= \sum_{l_8} \sum_{l_4^1} \sum_{l_4^2} \mathrm{P}_n\left(l_8, l_4^1, l_4^2\right) \prod_{j=1}^{2} \mathrm{Prob}\left(\left|A_4^j\right| = l_4^j\right). \tag{4.96}$$

From (4.94) to (4.95) we sum over all possible events. Then from (4.95) to (4.96) we rewrite the probability as the product of the probability of the cardinalities of $\left|A_4^j\right|$ for $j = 1, 2$ and their intersection.

Splitting $A_4^j$ into $A_2^{2j-1}$ and $A_2^{2j}$ for $j = 1, 2$ we have (4.96) become

$$\begin{aligned} &= \sum_{l_8} \sum_{l_4^1} \sum_{l_4^2} \mathrm{P}_n\left(l_8, l_4^1, l_4^2\right) \times \\ &\prod_{j=1}^{2} \sum_{l_2^{2j-1}} \sum_{l_2^{2j}} \mathrm{P}_n\left(l_4^j, l_2^{2j-1}, l_2^{2j}\right) \cdot \mathrm{Prob}\left(\left|A_2^{2j-1}\right| = l_2^{2j-1}\right) \cdot \mathrm{Prob}\left(\left|A_2^{2j}\right| = l_2^{2j}\right) \qquad (4.97) \\ &= \sum_{l_8} \sum_{l_4^1} \sum_{l_4^2} \mathrm{P}_n\left(l_8, l_4^1, l_4^2\right) \left( \sum_{l_2^1} \sum_{l_2^2} \mathrm{P}_n\left(l_4^1, l_2^1, l_2^2\right) \prod_{j=1}^{2} \mathrm{P}_n\left(l_2^j, d, d\right) \right) \\ &\times \left( \sum_{l_2^3} \sum_{l_2^4} \mathrm{P}_n\left(l_4^2, l_2^3, l_2^4\right) \prod_{j=3}^{4} \mathrm{P}_n\left(l_2^j, d, d\right) \right). \qquad (4.98) \end{aligned}$$

From (4.97) to (4.98) we repeat the process of rewriting the probability of the cardinality of the parent set as the product of the probabilities of the cardinalities of the two children and their intersection.

Next we upper bound $\mathrm{P}_n(\cdot)$ using its definition in Lemma 4.3.3 by products of polynomials and exponentials from the Stirling's formula to have (4.98) upper bounded by the following.

$$\begin{aligned} &\sum_{l_8} \sum_{l_4^1} \sum_{l_4^2} \pi\left(l_8, l_4^1, l_4^2\right) \cdot e^{\psi_n\left(l_8, l_4^1, l_4^2\right)} \times \\ &\left( \sum_{l_2^1} \sum_{l_2^2} \pi\left(l_4^1, l_2^1, l_2^2\right) \cdot e^{\psi_n\left(l_4^1, l_2^1, l_2^2\right)} \prod_{j=1}^{2} \pi\left(l_2^j, d, d\right) \cdot e^{\psi_n\left(l_2^j, d, d\right)} \right) \times \\ &\left( \sum_{l_2^3} \sum_{l_2^4} \pi\left(l_4^2, l_2^3, l_2^4\right) \cdot e^{\psi_n\left(l_4^2, l_2^3, l_2^4\right)} \prod_{j=3}^{4} \pi\left(l_2^j, d, d\right) \cdot e^{\psi_n\left(l_2^j, d, d\right)} \right) \qquad (4.99) \\ &= \sum_{l_8} \sum_{l_4^1} \sum_{l_4^2} \pi_8 \cdot \exp\left[\psi_n\left(l_8, l_4^1, l_4^2\right)\right] \times \\ &\left( \sum_{l_2^1} \sum_{l_2^2} \pi_4^1 \cdot \pi_2^1 \cdot \pi_2^2 \cdot \exp\left[\psi_n\left(l_4^1, l_2^1, l_2^2\right) + \psi_n\left(l_2^1, d, d\right) + \psi_n\left(l_2^2, d, d\right)\right] \right) \times \\ &\left( \sum_{l_2^3} \sum_{l_2^4} \pi_4^2 \cdot \pi_2^3 \cdot \pi_2^4 \cdot \exp\left[\psi_n\left(l_4^2, l_2^3, l_2^4\right) + \psi_n\left(l_2^3, d, d\right) + \psi_n\left(l_2^4, d, d\right)\right] \right) \qquad (4.100) \end{aligned}$$

where $\pi_8 = \pi\left(l_8, l_4^1, l_4^2\right)$, $\pi_4^j = \pi\left(l_4^j, l_2^{2j-1}, l_2^{2j}\right)$ for $j = 1, 2$ and $\pi_2^j = \pi\left(l_2^j, d, d\right)$ for $j = 1, \ldots, 4$. From (4.99) to (4.100) we collect like terms.

Now we decompose the first exponent, $\psi_n\left(l_8,l_4^1,l_4^2\right)$ into a sum of two parts, $\frac{1}{2}\psi_n\left(l_8,l_4^1,l_4^2\right)$ and $\frac{1}{2}\psi_n\left(l_8,l_4^1,l_4^2\right)$. Then we place one of the these two parts into the second and third exponential terms to have (4.100) become

$$\begin{aligned}
&\sum_{l_8}\sum_{l_4^1}\sum_{l_4^2}\pi_8\cdot\left(\sum_{l_2^1}\sum_{l_2^2}\pi_4^1\cdot\pi_2^1\cdot\pi_2^2\cdot\exp\left[\frac{1}{2}\cdot\psi_n\left(l_8,l_4^1,l_4^2\right)+\psi_n\left(l_4^1,l_2^1,l_2^2\right)\right.\right.\\
&\left.\left.+\psi_n\left(l_2^1,d,d\right)+\psi_n\left(l_2^2,d,d\right)\right]\right)\cdot\left(\sum_{l_2^3}\sum_{l_2^4}\pi_4^2\cdot\pi_2^3\cdot\pi_2^4\cdot\exp\left[\frac{1}{2}\psi_n\left(l_8,l_4^1,l_4^2\right)\right.\right.\\
&\left.\left.+\psi_n\left(l_4^2,l_2^3,l_2^4\right)+\psi_n\left(l_2^3,d,d\right)+\psi_n\left(l_2^4,d,d\right)\right]\right). \qquad (4.101)
\end{aligned}$$

Let's say the two exponents in (4.101) are maximized at $\bar{l}_8,\bar{l}_4^1,\bar{l}_4^2,\bar{l}_2^j$, and $\hat{l}_8,\hat{l}_4^1,\hat{l}_4^2,\hat{l}_2^j$, for $j=1,\ldots,4$ respectively. Since each is symmetric their maximum must occur at the same point, $(a_8,a_4,a_2,d)$ where $\bar{l}_8=\hat{l}_8=a_8$, $\bar{l}_4^1=\bar{l}_4^2=\hat{l}_4^1=\hat{l}_4^2=a_4$ and $\bar{l}_2^1=\bar{l}_2^2=\bar{l}_2^3=\bar{l}_2^4=\hat{l}_2^1=\hat{l}_2^2=\hat{l}_2^3=\hat{l}_2^4=a_2$. Therefore, we can upper bound (4.101) by the following

$$\exp\left[\Psi_n\left(a_8,a_4,a_2,d\right)\right]\cdot\sum_{l_8}\sum_{l_4^1,l_4^2}\pi_8\cdot\left(\sum_{l_2^1,l_2^2}\pi_4^1\cdot\pi_2^1\cdot\pi_2^2\right)\cdot\left(\sum_{l_2^3,l_2^4}\pi_4^2\cdot\pi_2^3\cdot\pi_2^4\right), \qquad (4.102)$$

where

$$\Psi_n\left(a_8,a_4,a_2,d\right)=\psi_n\left(a_8,a_4,a_4\right)+2\cdot\psi_n\left(a_4,a_2,a_2\right)+4\cdot\psi_n\left(a_2,d,d\right). \qquad (4.103)$$

Now we focus on bounding the following term

$$\sum_{l_8}\sum_{l_4^1,l_4^2}\pi_8\cdot\left(\sum_{l_2^1,l_2^2}\pi_4^1\cdot\pi_2^1\cdot\pi_2^2\right)\cdot\left(\sum_{l_2^3,l_2^4}\pi_4^2\cdot\pi_2^3\cdot\pi_2^4\right). \qquad (4.104)$$

We start by bounding the rightmost bracket in (4.104) by considering the largest possible range of the limits of the sum, hence

$$\begin{aligned}
\sum_{l_2^3,l_2^4}\pi_4^2\cdot\pi_2^3\cdot\pi_2^4 &\le \sum_{l_2^3=d}^{2d}\pi\left(l_2^3,d,d\right)\cdot\sum_{l_2^4=d}^{2d}\pi\left(l_4^2,l_2^3,l_2^4\right)\cdot\pi\left(l_2^4,d,d\right), && (4.105)\\
&< \pi\left(d,d,d\right)\cdot\sum_{l_2^4=d}^{2d}\sum_{l_2^3=d}^{2d}\pi\left(l_4^2,l_2^3,l_2^4\right)\cdot\pi\left(l_2^3,d,d\right), && (4.106)\\
&< \left[\pi\left(d,d,d\right)\right]^2\cdot\sum_{l_2^4=d}^{2d}\sum_{l_2^3=d}^{2d}\pi\left(l_4^2,l_2^3,l_2^4\right). && (4.107)
\end{aligned}$$

From (4.105) to (4.106) we maximize $\pi\left(l_2^4,d,d\right)$ at $l_2^4=d$ using (4.61) and factor it out. We repeat the same process for (4.106) to (4.107) for $\pi\left(l_2^3,d,d\right)$.

Similarly, we can upper the other bracket in (4.104) as thus

$$\sum_{l_2^1,l_2^2} \pi_4^1 \cdot \pi_2^1 \cdot \pi_2^2 < \left[\pi\left(d,d,d\right)\right]^2 \cdot \sum_{l_2^2=d}^{2d} \sum_{l_2^1=d}^{2d} \pi\left(l_4^1, l_2^1, l_2^2\right). \tag{4.108}$$

Combining (4.107) and (4.108) we have an upper bound on the product of the two brackets in (4.104) as

$$\left[\pi\left(d,d,d\right)\right]^4 \cdot \left( \sum_{l_2^2=d}^{2d} \sum_{l_2^1=d}^{2d} \pi\left(l_4^1, l_2^1, l_2^2\right) \right) \cdot \left( \sum_{l_2^4=d}^{2d} \sum_{l_2^3=d}^{2d} \pi\left(l_4^2, l_2^3, l_2^4\right) \right), \tag{4.109}$$

which is in turn bound above by

$$d^4 \cdot \left[\pi\left(d,d,d\right)\right]^4 \cdot \pi\left(l_4^1, 2d, 2d\right) \cdot \pi\left(l_4^2, 2d, 2d\right). \tag{4.110}$$

From (4.109) to (4.110) we upper bound $\pi\left(l_4^2, l_2^3, l_2^4\right)$ and $\pi\left(l_4^1, l_2^1, l_2^2\right)$ by $\pi\left(l_4^2, 2d, 2d\right)$ and $\pi\left(l_4^1, 2d, 2d\right)$ respectively considering the fact that the minimum possible value of $l_4^j$ for $j = 1, 2$ is $2d$.

Therefore we bound the whole of (4.104) by

$$d^4 \cdot \left[\pi\left(d,d,d\right)\right]^4 \cdot \sum_{l_8} \sum_{l_4^1,l_4^2} \pi_8 \cdot \pi\left(l_4^1, 2d, 2d\right) \cdot \pi\left(l_4^2, 2d, 2d\right), \tag{4.111}$$

$$< d^4 \cdot \left[\pi\left(d,d,d\right)\right]^4 \cdot \sum_{l_8} \pi_8 \sum_{l_4^1=2d}^{4d} \pi\left(l_4^1, 2d, 2d\right) \sum_{l_4^2=2d}^{4d} \pi\left(l_4^2, 2d, 2d\right), \tag{4.112}$$

$$< d^4 \cdot \left[\pi\left(d,d,d\right)\right]^4 \cdot (2d)^2 \cdot \left[\pi\left(2d,2d,2d\right)\right]^2 \cdot \sum_{l_8=4d}^{8d} \pi\left(l_8, 4d, 4d\right), \tag{4.113}$$

$$< d^4 \cdot \left[\pi\left(d,d,d\right)\right]^4 \cdot (2d)^2 \cdot \left[\pi\left(2d,2d,2d\right)\right]^2 \cdot 4d \cdot \pi\left(4d, 4d, 4d\right). \tag{4.114}$$

We upper bound (4.111) by (4.112) by considering the maximum possible range of the summation over $l_4^1$ and $l_4^2$. From (4.112) to (4.113) we upper bound the last two sums by evaluating $\pi(\cdot)$ and the smallest values of the summations and multiply this by the number of the terms in the sums. We repeat the same process from (4.113) to (4.114).

Now we use (4.61) to evaluate $\pi(\cdot)$ in (4.114) to bound (4.114) by the following.

$$d^4 \cdot \left[\left(\frac{5}{4}\right)^2 \sqrt{2\pi d}\right]^4 \cdot (2d)^2 \cdot \left[\left(\frac{5}{4}\right)^2 \sqrt{2^2\pi d}\right]^2 \cdot 4d \cdot \left[\left(\frac{5}{4}\right)^2 \sqrt{2^3\pi d}\right], \tag{4.115}$$

$$= \left(\frac{5}{4}\right)^{14} d^{21/2} \cdot 4^4 \pi^3 \cdot 2\sqrt{2\pi} \tag{4.116}$$

$$= \frac{2}{25\sqrt{2\pi\left(8^3\right)d^3}} \cdot \frac{25\sqrt{2\pi\left(8^3\right)d^3}}{2} \cdot \left(\frac{5}{4}\right)^{14} d^{21/2} \cdot 4^4 \pi^3 \cdot 2\sqrt{2\pi} \tag{4.117}$$

$$< \frac{2}{25\sqrt{2\pi\left(8^3\right)d^3}} \cdot (5d)^{24} \tag{4.118}$$

$$= \frac{2}{25\sqrt{2\pi\left(8^3\right)d^3}} \cdot \exp\left[24\log\left(5d\right)\right]. \tag{4.119}$$

From (4.115) to (4.116) we simplify and we multiply (4.116) by $\frac{2}{25\sqrt{2\pi(8^3)d^3}}$ and its reciprocal to get (4.117). Then from (4.117) to (4.118) we upper bound the factor multiplying $\frac{2}{25\sqrt{2\pi(8^3)d^3}}$ in (4.117) by $(5d)^{24}$ then we rewrote $(5d)^{24}$ as $\exp\left[24\log\left(5d\right)\right]$ to get the expression in (4.119).

Using (4.119) we can upper bound (4.102) by

$$\frac{2}{25\sqrt{2\pi\left(8^3\right)d^3}} \cdot \exp\left[24\log\left(5d\right) + \Psi_n\left(a_8, a_4, a_2, d\right)\right]. \tag{4.120}$$

The expression (4.120) is in the right format and consistent with Theorem 4.2.4 with polynomial $p_{max}(s,d) = \frac{2}{25\sqrt{2\pi(8^3)d^3}}$ and $\Psi\left(a_8, a_4, a_2, d\right) = \frac{1}{n}\left[24\log\left(5d\right) + \Psi_n\left(a_8, a_4, a_2, d\right)\right]$ for the case $s = 8$ where $\Psi_n\left(a_8, a_4, a_2, d\right)$ given by (4.103).

### 4.5.2 Theorem 4.2.4 for Large $s$

By the dyadic splitting $|A_s| = \left|A^1_{\lceil\frac{s}{2}\rceil} \cup A^2_{\lfloor\frac{s}{2}\rfloor}\right|$ and therefore

$$\begin{aligned}
\text{Prob}\left(|A_s| \leq a_s\right) &= \text{Prob}\left(\left|A^1_{\lceil\frac{s}{2}\rceil} \cup A^2_{\lfloor\frac{s}{2}\rfloor}\right| \leq a_s\right) && (4.121)\\
&= \sum_{l_s=\min\left(l_{\lceil\frac{s}{2}\rceil}, l_{\lfloor\frac{s}{2}\rfloor}\right)}^{\min\left(2\min\left(l_{\lceil\frac{s}{2}\rceil}, l_{\lfloor\frac{s}{2}\rfloor}\right), a_s\right)} \quad \sum_{l^j_{\lceil\frac{s}{2}\rceil}=\min\left(l_{\lceil\frac{s}{2^2}\rceil}, l_{\lfloor\frac{s}{2^2}\rfloor}\right)_{j=1,2}}^{\min\left(2\min\left(l_{\lceil\frac{s}{2^2}\rceil}, l_{\lfloor\frac{s}{2^2}\rfloor}\right), l_s\right)} \text{Prob}\left(\left|A^1_{\lceil\frac{s}{2}\rceil} \cup A^2_{\lfloor\frac{s}{2}\rfloor}\right| = l_s\right) && (4.122)\\
&= \sum_{l_s}\sum_{l^1_{\lceil\frac{s}{2}\rceil}}\sum_{l^2_{\lfloor\frac{s}{2}\rfloor}} \text{P}_n\left(l_s, l^1_{\lceil\frac{s}{2}\rceil}, l^2_{\lfloor\frac{s}{2}\rfloor}\right) \text{Prob}\left(\left|A^1_{\lceil\frac{s}{2}\rceil}\right| = l^1_{\lceil\frac{s}{2}\rceil}\right) \text{Prob}\left(\left|A^2_{\lfloor\frac{s}{2}\rfloor}\right| = l^2_{\lfloor\frac{s}{2}\rfloor}\right). && (4.123)
\end{aligned}$$

From (4.121) to (4.122) we sum over all possible events while from (4.122) to (4.123), in line with the splitting technique, we simplify the probability to the product of the probabilities of the cardinalities of $\left|A^1_{\lceil\frac{s}{2}\rceil}\right|$ and $\left|A^2_{\lfloor\frac{s}{2}\rfloor}\right|$ and their intersection.

In a slight abuse of notation we write $\sum_{l^j\, j=1,\ldots,x}$ to denote applying the sum $x$ times. Now we use Lemma 4.3.5 to simplify (4.123) as follows.

$$\begin{aligned}
&\sum_{\substack{l^{j_1}_{Q_0} \\ j_1=1,\ldots,q_0}} \sum_{\substack{l^{j_2}_{Q_1} \\ j_2=1,\ldots,q_1}} \sum_{\substack{l^{j_3}_{R_1} \\ j_3=1,\ldots,r_1}} \text{P}_n\left(l^{j_1}_{Q_0}, l^{2j_1-1}_{\lceil\frac{Q_0}{2}\rceil}, l^{2j_1}_{\lfloor\frac{Q_0}{2}\rfloor}\right)\\
&\qquad \times \prod_{j_2=1}^{q_1} \text{Prob}\left(\left|A^{j_2}_{Q_1}\right| = l^{j_2}_{Q_1}\right) \prod_{j_3=q_1+1}^{q_1+r_1} \text{Prob}\left(\left|A^{j_3}_{R_1}\right| = l^{j_3}_{R_1}\right). \qquad (4.124)
\end{aligned}$$

Let's quickly verify that (4.124) is the same as (4.123). By Lemma 4.3.5, $Q_0 = s$ is the number of columns in the set at the zeroth level of the split while $q_0 = 1$ is the number of sets with $Q_0$ columns at the zeroth level of the split. Thus for $j_1 = 1$ the first summation and the $\mathrm{P}_n(\cdot)$ term are the same in the two equations. If $\lceil \frac{Q_0}{2} \rceil = \lfloor \frac{Q_0}{2} \rfloor$, then they are both equal to $Q_1$ and $q_1 = 2$ while $r_1 = 0$. If on the other hand $\lceil \frac{Q_0}{2} \rceil = \lfloor \frac{Q_0}{2} \rfloor + 1$, then $q_1 = 1$ and $r_1 = 1$. In either case we have the remaining part of the expression of (4.123) i.e. the second two summations and the product of the two $\mathrm{Prob}(\cdot)$.

Now we proceed with the splitting - note (4.124) stopped only at the first level. At the next level, the second, we will have $q_2$ sets with $Q_2$ columns and $r_2$ sets with $R_2$ columns which leads to the following expression.

$$\begin{aligned}
&\sum_{\substack{l^{j_1}_{Q_0}\\ j_1=1,\dots,q_0}} \sum_{\substack{l^{j_2}_{Q_1}\\ j_2=1,\dots,q_1}} \sum_{\substack{l^{j_3}_{R_1}\\ j_3=1,\dots,r_1}} \mathrm{P}_n\left(l^{j_1}_{Q_0}, l^{2j_1-1}_{\lceil \frac{Q_0}{2}\rceil}, l^{2j_1}_{\lfloor \frac{Q_0}{2}\rfloor}\right) \times \\
&\qquad \Bigg[ \sum_{\substack{l^{j_4}_{Q_2}\\ j_4=1,\dots,q_2}} \sum_{\substack{l^{j_5}_{R_2}\\ j_5=1,\dots,r_2}} \mathrm{P}_n\left(l^{j_2}_{Q_1}, l^{2j_2-1}_{\lceil \frac{Q_1}{2}\rceil}, l^{2j_2}_{\lfloor \frac{Q_1}{2}\rfloor}\right) \mathrm{P}_n\left(l^{j_3}_{R_1}, l^{2j_3-1}_{\lceil \frac{R_1}{2}\rceil}, l^{2j_3}_{\lfloor \frac{R_1}{2}\rfloor}\right) \\
&\qquad\qquad \times \prod_{j_4=1}^{q_2} \mathrm{Prob}\left(\left|A^{j_4}_{Q_1}\right| = l^{j_4}_{Q_1}\right) \prod_{j_5=q_2+1}^{q_2+r_2} \mathrm{Prob}\left(\left|A^{j_5}_{R_1}\right| = l^{j_5}_{R_1}\right)\Bigg].
\end{aligned} \tag{4.125}$$

We continue this splitting of each instance of $\mathrm{Prob}(\cdot)$ for $\lceil \log_2 s \rceil - 1$ levels until reaching sets with single columns where, by construction, the probability that the single column has $d$ nonzeros is one. This process gives a complicated product of nested sums of $\mathrm{P}_n(\cdot)$ which we express as

$$\begin{aligned}
&\sum_{\substack{l^{j_1}_{Q_0}\\ j_1=1,\dots,q_0}} \sum_{\substack{l^{j_2}_{Q_1}\\ j_2=1,\dots,q_1}} \sum_{\substack{l^{j_3}_{R_1}\\ j_3=1,\dots,r_1}} \mathrm{P}_n\left(l^{j_1}_{Q_0}, l^{2j_1-1}_{\lceil \frac{Q_0}{2}\rceil}, l^{2j_1}_{\lfloor \frac{Q_0}{2}\rfloor}\right) \times \\
&\quad \Bigg[ \sum_{\substack{l^{j_4}_{Q_2}\\ j_4=1,\dots,q_2}} \sum_{\substack{l^{j_5}_{R_2}\\ j_5=1,\dots,r_2}} \mathrm{P}_n\left(l^{j_2}_{Q_1}, l^{2j_2-1}_{\lceil \frac{Q_1}{2}\rceil}, l^{2j_2}_{\lfloor \frac{Q_1}{2}\rfloor}\right) \mathrm{P}_n\left(l^{j_3}_{R_1}, l^{2j_3-1}_{\lceil \frac{R_1}{2}\rceil}, l^{2j_3}_{\lfloor \frac{R_1}{2}\rfloor}\right) \times \Bigg[ \cdots \\
&\quad \times \Bigg[ \sum_{\substack{l^{j_{2\lceil \log_2 s\rceil-2}}_{Q_{\lceil \log_2 s\rceil-1}}\\ j_{2\lceil \log_2 s\rceil-2}=1,\dots,q_{j_{\lceil \log_2 s\rceil-1}}}} \mathrm{P}_n\left(l_4^{j_{2\lceil \log_2 s\rceil-4}}, l_2^{2j_{2\lceil \log_2 s\rceil-4}-1}, l_2^{2j_{2\lceil \log_2 s\rceil-4}}\right) \\
&\qquad\qquad \times \mathrm{P}_n\left(l_3^{j_{2\lceil \log_2 s\rceil-3}}, l_2^{2j_{2\lceil \log_2 s\rceil-3}-1}, d\right) \cdot \mathrm{P}_n\left(l_2^{j_{2\lceil \log_2 s\rceil-2}}, d, d\right)\Bigg] \cdots \Bigg].
\end{aligned} \tag{4.126}$$

Using the definition of $\mathrm{P}_n(\cdot)$ in Lemma 4.3.3 we bound (4.126) by bounding each $\mathrm{P}_n(\cdot)$ as in (4.57) with a product of a polynomial, $\pi(\cdot)$, and an exponential with exponent $\psi_n(\cdot)$.

$$\begin{aligned}
&\sum_{\substack{l_{Q_0}^{j_1}\\ j_1=1,\ldots,q_0}} \sum_{\substack{l_{Q_1}^{j_2}\\ j_2=1,\ldots,q_1}} \sum_{\substack{l_{R_1}^{j_3}\\ j_3=1,\ldots,r_1}} \pi\left(l_{Q_0}^{j_1}, l_{\lceil\frac{Q_0}{2}\rceil}^{2j_1-1}, l_{\lfloor\frac{Q_0}{2}\rfloor}^{2j_1}\right)\cdot e^{\psi_n\left(l_{Q_0}^{j_1}, l_{\lceil\frac{Q_0}{2}\rceil}^{2j_1-1}, l_{\lfloor\frac{Q_0}{2}\rfloor}^{2j_1}\right)} \\
&\quad\cdot\Bigg[\sum_{\substack{l_{Q_2}^{j_4}\\ j_4=1,\ldots,q_2}} \sum_{\substack{l_{R_2}^{j_5}\\ j_5=1,\ldots,r_2}} \pi\left(l_{Q_1}^{j_2}, l_{\lceil\frac{Q_1}{2}\rceil}^{2j_2-1}, l_{\lfloor\frac{Q_1}{2}\rfloor}^{2j_2}\right)\cdot e^{\psi_n\left(l_{Q_1}^{j_2}, l_{\lceil\frac{Q_1}{2}\rceil}^{2j_2-1}, l_{\lfloor\frac{Q_1}{2}\rfloor}^{2j_2}\right)} \\
&\quad\times\pi\left(l_{R_1}^{j_3}, l_{\lceil\frac{R_1}{2}\rceil}^{2j_3-1}, l_{\lfloor\frac{R_1}{2}\rfloor}^{2j_3}\right)\cdot e^{\psi_n\left(l_{R_1}^{j_3}, l_{\lceil\frac{R_1}{2}\rceil}^{2j_3-1}, l_{\lfloor\frac{R_1}{2}\rfloor}^{2j_3}\right)} \times\Bigg[\ldots\times\Bigg[ \\
&\quad\sum_{\substack{l_{Q_{\lceil\log_2 s\rceil-1}}^{j_{2\lceil\log_2 s\rceil-2}}\\ j_{2\lceil\log_2 s\rceil-2}=1,\ldots,q_{j_{\lceil\log_2 s\rceil-1}}}} \pi\left(l_4^{j_{2\lceil\log_2 s\rceil-4}}, l_2^{2j_{2\lceil\log_2 s\rceil-4}-1}, l_2^{2j_{2\lceil\log_2 s\rceil-4}}\right) \\
&\quad\times e^{\psi_n\left(l_4^{j_{2\lceil\log_2 s\rceil-4}}, l_2^{2j_{2\lceil\log_2 s\rceil-4}-1}, l_2^{2j_{2\lceil\log_2 s\rceil-4}}\right)}\cdot\pi\left(l_3^{j_{2\lceil\log_2 s\rceil-3}}, l_2^{2j_{2\lceil\log_2 s\rceil-3}-1}, d\right) \\
&\quad e^{\psi_n\left(l_3^{j_{2\lceil\log_2 s\rceil-3}}, l_2^{2j_{2\lceil\log_2 s\rceil-3}-1}, d\right)}\cdot\pi\left(l_2^{j_{2\lceil\log_2 s\rceil-2}}, d, d\right)\cdot e^{\psi_n\left(l_2^{j_{2\lceil\log_2 s\rceil-2}}, d, d\right)}\Bigg]\ldots\Bigg].
\end{aligned} \tag{4.127}$$

Using Lemma 4.3.6 we maximize the $\psi_n(\cdot)$ and hence the exponentials. If we maximize each by choosing $l_{(\cdot)}$ to be $a_{(\cdot)}$, then we can pull the exponentials out of the product. The exponential will then have the exponent $\Psi_n\left(a_s,\ldots,a_2,d\right)$. The factor involving the $\pi(\cdot)$ will be called $\Pi\left(l_s,\ldots,l_2,d\right)$ and we have the following upper bound for (4.127).

$$\Pi\left(l_s,\ldots,l_2,d\right)\cdot\exp\left[\Psi_n\left(a_s,\ldots,a_2,d\right)\right], \tag{4.128}$$

where the exponent $\Psi_n\left(a_s,\ldots,a_2,d\right)$ is given by

$$\psi_n\left(a_{Q_0}, a_{\lceil\frac{Q_0}{2}\rceil}, a_{\lfloor\frac{Q_0}{2}\rfloor}\right)+\ldots+\psi_n\left(a_2,d,d\right). \tag{4.129}$$

Now we attempt to bound the probability of interest in (4.121). This task reduces to bounding $\Pi\left(l_s,\ldots,l_2,d\right)$ and $\Psi_n\left(a_s,\ldots,a_2,d\right)$ in (4.128) and we start with the former, i.e. bounding $\Pi\left(l_s,\ldots,l_2,d\right)$. We bound each sum of $\pi(\cdot)$ in $\Pi\left(l_s,\ldots,l_2,d\right)$ of (4.128) by the maximum of summations multiplied by the number of terms in the sum. From (4.61) we see that $\pi(\cdot)$ is maximized when all the three arguments are the same and using Corollary 4.3.11 we take largest possible arguments that are equal in the range of the summation. In this way the following proposition provides the bound we end up.

**Proposition 4.5.1.** *Let's make each summation over the sets with the same number of columns to have the same range where the range we take are the maximum possible for each such set. Let's also maximize $\pi(\cdot)$ where all its three input variables are equal and are equal to the maxi-*

*mum of the third variable. Then we bound each sum by the largest term in the sum multiplied by the number of terms. This scheme combined with Lemma 4.3.5 give the following bound.*

$$
\begin{aligned}
\Pi\left(l_s,\ldots,l_2,d\right) \le & \left(\left\lceil\frac{Q_0}{2}\right\rceil d\left(\frac{5}{4}\right)^2\sqrt{2\pi\left\lfloor\frac{Q_0}{2}\right\rfloor d}\right)^{q_0} \times \\
& \prod_{j=1}^{\lceil\log_2 s\rceil-2}\left(\left\lceil\frac{Q_j}{2}\right\rceil d\left(\frac{5}{4}\right)^2\sqrt{2\pi\left\lfloor\frac{Q_j}{2}\right\rfloor d}\right)^{q_j}\cdot\left(\left\lceil\frac{R_j}{2}\right\rceil d\left(\frac{5}{4}\right)^2\sqrt{2\pi\left\lfloor\frac{R_j}{2}\right\rfloor d}\right)^{r_j} \\
& \times\left(\left\lceil\frac{Q_{\lceil\log_2 s\rceil-1}}{2}\right\rceil d\left(\frac{5}{4}\right)^2\sqrt{2\pi\left\lfloor\frac{Q_{\lceil\log_2 s\rceil-1}}{2}\right\rfloor d}\right)^{p_{\lceil\log_2 s\rceil-1}}. \qquad (4.130)
\end{aligned}
$$

*Proof.* From (4.61) we have

$$
\pi(y,y,y)=\left(\frac{5}{4}\right)^2\sqrt{\frac{2\pi y(n-y)}{n}}<\left(\frac{5}{4}\right)^2\sqrt{2\pi y}. \qquad (4.131)
$$

Simply put, we bound $\sum_x \pi(x,y,z)$ by multiplying the maximum of $\pi(x,y,z)$ with the number of terms in the summation. Remember the order of magnitude of the arguments of $\pi(x,y,z)$ is $x\ge y\ge z$. Therefore, the maximum of $\pi(x,y,z)$ occurs when the arguments are all equal to the maximum value of $z$. In our splitting scheme the maximum possible value of $l_{\left\lfloor\frac{Q_j}{2}\right\rfloor}$ is $\left\lfloor\frac{Q_j}{2}\right\rfloor\cdot d$ since there are $d$ nonzeros in each column. Also $l_{\left\lfloor\frac{Q_j}{2}\right\rfloor}\le l_{Q_j}\le l_{\left\lfloor\frac{Q_j}{2}\right\rfloor}+l_{\left\lceil\frac{Q_j}{2}\right\rceil}$ so the number of terms in the summation over $l_{Q_j}$ is $\left\lceil\frac{Q_j}{2}\right\rceil\cdot d$, and similarly for $R_j$. We know the values of the $Q_j$ and the $R_j$ and their quantities $q_j$ and $r_j$ respectively from Lemma 4.3.5.

We replace $y$ by $\left\lfloor\frac{Q_j}{2}\right\rfloor\cdot d$ or $\left\lfloor\frac{R_j}{2}\right\rfloor\cdot d$ accordingly into the bound of $\pi(y,y,y)$ in (4.131) and multiply by the number of terms in the summation, i.e. $\left\lceil\frac{Q_j}{2}\right\rceil\cdot d$ or $\left\lceil\frac{R_j}{2}\right\rceil\cdot d$. This product is then repeated $q_j$ or $r_j$ times accordingly until the last level of the split, $j=\lceil\log_2 s\rceil-1$, where we have $q_{\lceil\log_2 s\rceil-1}$ and $Q_{\lceil\log_2 s\rceil-1}$ (which is equal to 2). We exclude $R_{\lceil\log_2 s\rceil-1}$ since $l_{R_{\lceil\log_2 s\rceil-1}}=d$. Putting the whole product together results to (4.130) hence concluding the proof of Proposition 4.5.1. □

As a final step we need the following corollary.

**Corollary 4.5.2.**

$$
\Pi\left(l_s,\ldots,l_2,d\right)<\frac{2}{25\sqrt{2\pi s^3d^3}}\cdot\exp\left[3s\log(5d)\right]. \qquad (4.132)
$$

*Proof.* From Lemma 4.3.5 we can upper bound $R_j$ by $Q_j$ . Consequently (4.130) is upper bounded by the following.

$$
\begin{aligned}
&\left(\left\lceil\frac{Q_0}{2}\right\rceil d\left(\frac{5}{4}\right)^2\sqrt{2\pi\left\lfloor\frac{Q_0}{2}\right\rfloor d}\right)^{q_0}\cdot\prod_{j=1}^{\lceil\log_2 s\rceil-2}\left(\left\lceil\frac{Q_j}{2}\right\rceil d\left(\frac{5}{4}\right)^2\sqrt{2\pi\left\lfloor\frac{Q_j}{2}\right\rfloor d}\right)^{q_j+r_j}\times \\
&\left(\left\lceil\frac{Q_{\lceil\log_2 s\rceil-1}}{2}\right\rceil d\left(\frac{5}{4}\right)^2\sqrt{2\pi\left\lfloor\frac{Q_{\lceil\log_2 s\rceil-1}}{2}\right\rfloor d}\right)^{q_{\lceil\log_2 s\rceil-1}} \qquad (4.133)
\end{aligned}
$$

Now we use the property that $q_j + r_j = 2^j$ for $j = 1, \ldots, \lceil \log_2 s \rceil - 1$ from Lemma 4.3.5 to bound (4.133) by the following.

$$\prod_{j=0}^{\lceil \log_2 s \rceil - 1} \left( \left\lceil \frac{Q_j}{2} \right\rceil d \left( \frac{5}{4} \right)^2 \sqrt{2\pi \left\lfloor \frac{Q_j}{2} \right\rfloor d} \right)^{2^j}. \tag{4.134}$$

We have a strict upper bound when $r_{\lceil \log_2 s \rceil - 1} \neq 0$, which occurs when $s$ is not a power of 2, because then by $q_j + r_j = 2^j$ we have $q_{\lceil \log_2 s \rceil - 1} + r_{\lceil \log_2 s \rceil - 1} = 2^{\lceil \log_2 s \rceil - 1}$. In fact (4.134) is an overestimate for a large $s$ which is not a power of 2.

Note $Q_j = \left\lceil \frac{s}{2^j} \right\rceil$ by Lemma 4.3.5. Thus $\left\lceil \frac{Q_j}{2} \right\rceil = \left\lceil \frac{s}{2^{j+1}} \right\rceil$ and $\left\lfloor \frac{Q_j}{2} \right\rfloor \leq \left\lceil \frac{s}{2^{j+1}} \right\rceil$. So we bound (4.134) by the following.

$$\prod_{j=0}^{\lceil \log_2 s \rceil - 1} \left( \left\lceil \frac{s}{2^{j+1}} \right\rceil d \left( \frac{5}{4} \right)^2 \sqrt{2\pi \left\lceil \frac{s}{2^{j+1}} \right\rceil d} \right)^{2^j} \tag{4.135}$$

Next we upper bound $\lceil \log_2 s \rceil - 1$ in the limit of the product by $\log_2 s$ and upper bound $\left\lceil \frac{s}{2^{j+1}} \right\rceil$ by $\frac{s}{2^{j+1}} + \frac{1}{2} = \frac{s}{2^{j+1}} \left( 1 + \frac{2^{j+1}}{s} \right)$, we also move the $d$ into the square root and combined the constants to have the following bound on (4.135).

$$\prod_{j=0}^{\log_2 s} \left[ \frac{s}{2^{j+1}} \left( 1 + \frac{2^{j+1}}{s} \right) \left( \frac{25\sqrt{2\pi}}{16} \right) \cdot \sqrt{\frac{s}{2^{j+1}} \left( 1 + \frac{2^{j+1}}{s} \right) d^3} \right]^{2^j}. \tag{4.136}$$

We bound $\left( 1 + \frac{2^{j+1}}{s} \right)$ by 2 to bound the above by

$$\prod_{j=0}^{\log_2 s} \left[ \frac{s}{2^j} \left( \frac{25\sqrt{2\pi}}{16} \right) \sqrt{\frac{s}{2^j} d^3} \right]^{2^j} = \prod_{j=0}^{\log_2 s} \left[ \left( \frac{25\sqrt{2\pi}}{16} \right) \sqrt{\frac{s^3 d^3}{2^{3j}}} \right]^{2^j} \tag{4.137}$$

where we moved $s/2^j$ into the square root. Using the rule of indices the product of the constant term is replaced by its power to sum of the indices. We then rearranged to have the power 3/2 in the outside and this gives the following.

$$\left( \frac{25\sqrt{2\pi}}{16} \right)^{\sum_{i=0}^{\log_2 s} 2^i} \left[ \prod_{j=0}^{\log_2 s} \left( \frac{sd}{2^j} \right)^{2^j} \right]^{3/2} \tag{4.138}$$

$$= \left( \frac{25\sqrt{2\pi}}{16} \right)^{2s-1} \left[ (sd)^{\sum_{i=0}^{\log_2 s} 2^i} \prod_{j=0}^{\log_2 s} \left( \frac{1}{2^j} \right)^{2^j} \right]^{3/2} \tag{4.139}$$

$$= \left( \frac{25\sqrt{2\pi}}{16} \right)^{2s-1} \left[ (sd)^{2s-1} \left( \frac{1}{2} \right)^{\sum_{j=0}^{\log_2 s} j 2^j} \right]^{3/2}. \tag{4.140}$$

From (4.138) to (4.139) we evaluate the power of the first factor which is a geometric series and we again use the rule of indices for the $sd$ factor. Then from (4.139) to (4.140) we use the indices' rule for the last factor and evaluate the power of the $sd$ factor which is also a geometric series. We simplify the power of the last factor by using the following.

$$\sum_{k=1}^{m} k \cdot 2^k = (m-1) \cdot 2^{m+1} + 2. \tag{4.141}$$

This therefore simplifies (4.140) as follows.

$$\begin{aligned}
&\left(\frac{25\sqrt{2\pi}}{16}\right)^{2s-1} \left[(sd)^{2s-1} \left(\frac{1}{2}\right)^{(\log_2 s-1)\cdot 2^{\log_2 s+1}+2}\right]^{3/2} && (4.142)\\
&= \left(\frac{25\sqrt{2\pi}}{16}\right)^{2s-1} \left[(sd)^{2s-1} \left(\frac{1}{2}\right)^{2s(\log_2 s-1)} \frac{1}{4}\right]^{3/2} && (4.143)\\
&= \left(\frac{25\sqrt{2\pi}}{16}\right)^{2s-1} \left[\frac{(sd)^{2s}}{4sd} 2^{-2s\log_2 s} 2^{2s}\right]^{3/2} && (4.144)\\
&= \left(\frac{25\sqrt{2\pi}}{16}\right)^{2s} \left(\frac{16}{25\sqrt{2\pi}}\right) \left[\frac{(2sd)^{2s}}{4sd} s^{-2s}\right]^{3/2} && (4.145)\\
&= \left(\frac{25\sqrt{2\pi}}{16}\right)^{2s} \left(\frac{16}{25\sqrt{2\pi}}\right) \left[\frac{(2d)^{2s}}{4sd}\right]^{3/2}. && (4.146)
\end{aligned}$$

From (4.142) through (4.144) we simplify using basic properties of indices and logarithms. While from (4.144) to (4.145) we incorporate $2^{2s}$ into the first factor inside the square brackets and we rewrite the first factor into a product of a power in $s$ and another without $s$. From (4.145) to (4.146) the $s^{2s}$ and $s^{-2s}$ cancel out.

Now we expand the square brackets in (4.146) to have (4.147) below.

$$\begin{aligned}
&\left(\frac{25\sqrt{2\pi}}{16}\right)^{2s} \left(\frac{16}{25\sqrt{2\pi}}\right) \frac{1}{8\sqrt{s^3d^3}} (2d)^{3s} && (4.147)\\
&= \left(\frac{25\sqrt{2\pi}}{16}\right)^{2s} (2d)^{3s} \frac{2}{25\sqrt{2\pi s^3 d^3}} && (4.148)\\
&= \frac{2}{25\sqrt{2\pi s^3 d^3}} \cdot \exp\left(3s\log\left(2\left(\frac{25\sqrt{2\pi}}{16}\right)^{2/3} d\right)\right) && (4.149)\\
&< \frac{2}{25\sqrt{2\pi s^3 d^3}} \cdot \exp\left[3s\log(5d)\right] && (4.150)
\end{aligned}$$

From (4.147) to (4.148) we simplify and from (4.148) to (4.149) we rewrite the powers as an exponential with a logarithmic exponent. Then from (4.149) to (4.150) we upper bound $2\left(\frac{25\sqrt{2\pi}}{16}\right)^{2/3}$ by 5 which gives the required format of a product of a polynomial and an exponential to conclude the proof of the corollary. □

With the bound in Corollary 4.5.2 we have completed the bounding of $\Pi\left(l_s,\ldots,l_2,d\right)$ in (4.128). Next we bound $\Psi_n\left(a_s,\ldots,a_2,d\right)$ which is given by (4.129). Lemma 4.3.5 gives the three arguments for each $\psi_n(\cdot)$ and the number of $\psi_n(\cdot)$ with the same arguments. Using this lemma we express $\Psi_n\left(a_s,\ldots,a_2,d\right)$ as

$$\sum_{j=0}^{\lceil\log_2(s)\rceil-2}\left[q_j\cdot\psi_n\left(a_{Q_j},a_{\left\lceil\frac{Q_j}{2}\right\rceil},a_{\left\lfloor\frac{Q_j}{2}\right\rfloor}\right)+r_j\cdot\psi_n\left(a_{R_j},a_{\left\lceil\frac{R_j}{2}\right\rceil},a_{\left\lfloor\frac{R_j}{2}\right\rfloor}\right)\right]+ q_{\lceil\log_2(s)\rceil-1}\cdot\psi_n\left(a_2,d,d\right). \quad (4.151)$$

Equation (4.151) is bounded above in Lemma 4.3.7 by the following.

$$\sum_{j=0}^{\lceil\log_2(s)\rceil-1} 2^j\cdot\psi_n\left(a_{Q_j},a_{\left\lfloor\frac{R_j}{2}\right\rfloor},a_{\left\lfloor\frac{R_j}{2}\right\rfloor}\right). \quad (4.152)$$

If we let the $a_{2i}=a_{Q_j}$ and $a_i=a_{\left\lfloor\frac{R_j}{2}\right\rfloor}$ we have (4.152) become $\sum_{i=1}^{\lceil s/2\rceil}\frac{s}{2i}\cdot\psi_n\left(a_{2i},a_i,a_i\right)$ which is equal to the the following.

$$\sum_{i=1}^{\lceil s/2\rceil}\frac{s}{2i}\left[a_i\cdot\mathrm{H}\left(\frac{a_{2i}-a_i}{a_i}\right)+(n-a_i)\cdot\mathrm{H}\left(\frac{a_{2i}-a_i}{n-a_i}\right)-n\cdot\mathrm{H}\left(\frac{a_i}{n}\right)\right]. \quad (4.153)$$

Now we combine the bound of $\Pi\left(l_s,\ldots,l_2,d\right)$ in (4.132) and the exponential whose exponent is the bound of $\Psi_n\left(a_s,\ldots,a_2,d\right)$ in (4.153) to get (4.2), the polynomial $p_{max}(s,d)=\frac{2}{25\sqrt{2\pi s^3d^3}}$, and (4.3), the exponent of the exponential $\Psi\left(a_s,\ldots,d\right)$ which is given by the sum of $3s\log\left(5d\right)$ and the right hand side of (4.153).

Lemma 4.3.8 gives the $a_i$ that maximize (4.153) and the systems (4.51) and (4.52) they satisfy depending on the constraints on $a_s$. Solving completely the system (4.51) gives $\hat{a}_i$ in (4.50) and (4.4) which are the expected values of the $a_i$. The system (4.5) is equivalent to (4.52) hence also proven in Lemma 4.3.8. This therefore concludes the proof Theorem 4.2.4.

### 4.5.3 Theorem 4.2.6

Theorem 4.2.6 simply says that if $A$ is from the class of matrices we consider in Definition 4.2.1, i.e. it is either the adjacency matrix of a lossless $(k,d,\epsilon)$-expander or the adjacency matrix of a lossless $(k,d,\epsilon)$-expander with random signs on the ones, then $A$ satisfies (1.10) with $\overline{L}(k,n,N;A)=2\epsilon$. The first case where $A$ is the adjacency matrix of a lossless $(k,d,\epsilon)$-expander has been proven in [15] by Berinde et. al., hence we will just do the proof for the second case.

We will use similar notation and method from [79, 80] used for the proof of $A$ being the adjacency matrix of an expander. In our case though $A$ is not only an expander but it has random signs.

The right hand side of (1.10) is shown to hold using the triangle inequality as follows. Consider $G(U, V, E)$ where $E$ is the set of edges and $e_{ij} = (x_i, y_j)$ is the edge that connects vertex $x_i$ to vertex $y_j$. Therefore,

$$\begin{aligned} \|Ax\|_1 &= \sum_{j=1}^{N} \left| \sum_{e_{ij} \in E} a_{ij} x_i \right| && (4.154) \\ &\leq \sum_{j=1}^{N} \left( \sum_{e_{ij} \in E} |a_{ij} x_i| \right) && (4.155) \\ &= \sum_{j=1}^{N} \left( \sum_{e_{ij} \in E} |x_i| \right) && (4.156) \\ &= d\|x\|_1. && (4.157) \end{aligned}$$

From (4.154) to (4.155) we apply the triangle inequality

$$|a + b| \leq |a| + |b|. \tag{4.158}$$

From (4.155) to (4.156) we use the fact that the $a_{ij}$ are either 1 or -1; while from (4.156) to (4.157) we use the fact that by summing over all $i$ and $j$ each of the $|x_i|$ will occur $d$ times in the summation.

For the proof of the lower bound or the left hand side of (1.10) let's first define

$$E' := \{e_{ij} \mid \exists\ i' < i \text{ with } e_{ij} \in E\}.$$

$E'$ is referred to as the *collision set* where the right vertices of the edges in this set are identical to preceding vertices if the edges are ordered in a lexicographical way. The following lemma is used in the argument to follow.

**Lemma 4.5.3** (Lemma 9, [15])**.** $\displaystyle\sum_{e_{ij} \in E'} |x_i| \leq \epsilon d \|x\|_1 \quad \forall x \in \chi^N.$

*Proof.* The proof of this lemma goes as follows, we define

$$T_i := \{e_{i'j} \in E' \text{ with } i' \leq i\} \quad \text{and} \quad t_i := |T_i|.$$

Conventionally, we set $t_0 = 0$ but note also that $t_1 = 0$ by the definition of $T_i$ and that by the expansion property of the graph for any $k' \leq k,\ t_{k'} \leq \epsilon d k'$. Now without loss of generality we order the components of $x$ in a non-increasing way, $|x_1| \geq |x_2| \geq \ldots \geq |x_N|$, since the left hand side of (1.10) does not change by changing the coordinates of $x$. Therefore, for $k'' > k,\ x_{k''} = 0$ since $x$ is $k-$sparse. For each $i$ there are $(t_i - t_{i-1})$ edges in $E'$ that are connected to it, thus

$$\begin{aligned}\sum_{e_{ij}\in E'} |x_i| &= \sum_{i=1}^{N} |x_i|\left(t_i - t_{i-1}\right) && (4.159)\\ &= \sum_{i\leq k} t_i\left(|x_i| - |x_{i+1}|\right) && (4.160)\\ &\leq \sum_{i\leq k} \epsilon di\left(|x_i| - |x_{i+1}|\right) && (4.161)\\ &= \epsilon d \sum_{i\leq k} |x_i| && (4.162)\\ &= \epsilon d\|x\|_1. && (4.163)\end{aligned}$$

From (4.159) to (4.160) we rearrange, while from (4.160) to (4.161) we use the expansion property of the graph. From (4.161) to (4.162) we simplify and from (4.162) to (4.163) we use the definition of the $\ell_1$ norm knowing that $x$ is $k-$sparse, thus proving the lemma. □

Now we show that the lower bound holds as follows.

$$\begin{aligned}\|Ax\|_1 &= \sum_{j=1}^{N}\left|\sum_{e_{ij}\in E} a_{ij}x_i\right| && (4.164)\\ &= \sum_{j=1}^{N}\left|\sum_{e_{ij}\in E'} a_{ij}x_i + \sum_{e_{ij}\notin E'} a_{ij}x_i\right| && (4.165)\\ &\geq \sum_{j=1}^{N}\left(|\sum_{e_{ij}\notin E'} a_{ij}x_i| - |\sum_{e_{ij}\in E'} a_{ij}x_i|\right) && (4.166)\\ &= \sum_{j=1}^{N}\left(|\sum_{e_{ij}\notin E'} a_{ij}x_i|\right) - \sum_{j=1}^{N}\left(|\sum_{e_{ij}\in E'} a_{ij}x_i|\right) && (4.167)\\ &\geq \sum_{e_{ij}\notin E'} |a_{ij}x_i| - \sum_{e_{ij}\in E'} |a_{ij}x_i|. && (4.168)\end{aligned}$$

From (4.164) to (4.165) we expand the sum based on the fact that the edges in $E$ can be grouped into those in $E'$ and those not in $E'$; while from (4.165) to (4.166) we lower bound using the property $|a+b| \geq |a| - |b|$. From (4.166) to (4.167) we expand the brackets using the distributive property of summation; while from (4.167) to (4.168) we rewrite the first term since for each $j$ there is only one edges not in $E'$, in other words for each $j$ we are summing only one item, and then we upper bound the second term using the triangle inequality, (4.158).

Next we simplify (4.168) using the fact that the $a_{ij}$ indexed by the edges in $E'$ are either 1 or -1 to get (4.169) below.

$$\|Ax\|_1 \geq \sum_{e_{ij}\notin E'} |x_i| - \sum_{e_{ij}\in E'} |x_i| \qquad (4.169)$$

$$= \sum_{e_{ij} \notin E'} |x_i| + \sum_{e_{ij} \in E'} |x_i| - 2 \sum_{e_{ij} \in E'} |x_i| \tag{4.170}$$

$$\geq \sum_{e_{ij} \in E} |x_i| - 2\epsilon d \|x\|_1 \tag{4.171}$$

$$= d\|x\|_1 - 2\epsilon d \|x\|_1 \tag{4.172}$$

$$= (1 - 2\epsilon) d \|x\|_1. \tag{4.173}$$

From (4.169) to (4.170) we rewrite the expression using $a - b = a + b - 2b$. Then from (4.170) to (4.171) we simplify the first two terms using the fact that the edges in $E'$ and their complement set combined give the edges in $E$ and we upper bound the last term using Lemma 4.5.3. From (4.171) to (4.172) we simplify the first term by noting that for each $i$, $x_i$ is repeated $d$ times in the summation and finally we simplify (4.172) to get (4.173) which was the target results, hence concluding the proof.

### 4.5.4 Main Corollaries

**Corollary 4.2.5**

Satisfying RIP-1 means that for any $s-$sparse vector $x$, $\|A_S x\|_1 \geq (1 - 2\epsilon) d \|x\|_1$ which also means the cardinality of the set of neighbours $|A_s| \geq (1 - \epsilon) ds$. Therefore

$$\text{Prob}\left(\|A_S x\|_1 \leq (1 - 2\epsilon) d \|x\|_1\right) \equiv \text{Prob}\left(|A_s| \leq (1 - \epsilon) ds\right). \tag{4.174}$$

This implies that $a_s = (1 - \epsilon) ds$ and since this is restricting $a_s$ to be less than its expected value given by (4.4), the rest of the $a_i$ satisfy the polynomial system (4.5). If there exists a solution then the $a_i$ would be functions of $s$, $d$ and $\epsilon$ which makes $\Psi\left(a_s, \ldots, a_2, d\right) = \Psi\left(s, d, \epsilon\right)$.

**Corollary 4.2.7**

Corollary 4.2.5 states that by fixing $S$ and the other parameters, then

$$\text{Prob}\left(\|A_S x\|_1 \leq (1 - 2\epsilon) d \|x\|_1\right) < p_{max}(s, d) \cdot \exp\left[n \cdot \Psi\left(s, d, \epsilon\right)\right]. \tag{4.175}$$

Corollary 4.2.7 considers any $S \subset [N]$ and since the matrices are basically adjacency matrices of lossless expanders we need to consider any $S \subset [N]$ such that $|S| \leq k$. Therefore our target is $\text{Prob}\left(\|Ax\|_1 \leq (1 - 2\epsilon) d \|x\|_1\right)$ which is bounded by a simple union bound over all $\binom{N}{s}$ $S$ sets and by treating each set $S$, of cardinality less than $k$, independent we sum over this probability to get the following bound.

$$\begin{aligned}
&\sum_{s=2}^{k}\binom{N}{s}\cdot\text{Prob}\left(\|A_Sx\|_1\leq(1-2\epsilon)d\|x\|_1\right) && (4.176)\\
&<\sum_{s=2}^{k}\binom{N}{s}\cdot p_{max}(s,d)\cdot\exp\left[n\cdot\Psi\left(s,d,\epsilon\right)\right] && (4.177)\\
&<\sum_{s=2}^{k}\left(\frac{5}{4}\right)^2\frac{1}{\sqrt{2\pi s\left(1-\frac{s}{N}\right)}}\cdot p_{max}(s,d)\cdot\exp\left[N\text{H}\left(\frac{s}{N}\right)+n\cdot\Psi\left(s,d,\epsilon\right)\right] && (4.178)\\
&<k\left(\frac{5}{4}\right)^2\frac{p_{max}(k,d)}{\sqrt{2\pi k\left(1-\frac{k}{N}\right)}}\cdot\exp\left[N\left(\text{H}\left(\frac{k}{N}\right)+\frac{n}{N}\cdot\Psi\left(k,d,\epsilon\right)\right)\right]. && (4.179)
\end{aligned}$$

From (4.176) to (4.177) we bound the probability in (4.176) using Corollary 4.2.5. Then from (4.177) to (4.178) we bound $\binom{N}{s}$ using Stirling's formula (2.11) by a polynomial in $N$ multiplying $p_{max}(s,d)$ and an exponential incorporated into the exponent of the exponential term. From (4.178) to (4.179) using the fact that $N>2k$ which means $\text{H}\left(\frac{s}{N}\right)$ is largest when $s=k$ and being cognizant of the fact that the exponential is dominant we bound the summation by taking the maximum value of $s$ and multiplying by the number of terms plus one, giving $k$, in the summation. This gives $p'_{max}(N,k,d)=k\left(\frac{5}{4}\right)^2\frac{p_{max}(k,d)}{\sqrt{2\pi k\left(1-\frac{k}{N}\right)}}$ which simplifies to $\frac{1}{16\pi k\sqrt{2d^3\left(1-\frac{k}{N}\right)}}$ and the factor multiplying $N$ in the exponent $\Psi_{net}\left(k,n,N;d,\epsilon\right)=\text{H}\left(\frac{k}{N}\right)+\frac{n}{N}\cdot\Psi\left(k,d,\epsilon\right)$ as required.

### Corollary 4.2.8

Corollary 4.2.7 has given us an upper bound on the probability $\text{Prob}\left(\|Ax\|_1\leq(1-2\epsilon)d\|x\|_1\right)$ in (4.7). In this bound the exponential dominates the polynomial. Consequently, in the limit as $(k,n,N)\to\infty$ while $k/n\to\rho\in(0,1)$ and $n/N\to\delta\in(0,1)$ this bound blows up or it decays to zero. It blows up when $\Psi_{net}\left(k,n,N;d,\epsilon\right)$, which is the factor multiplying $N$ in the exponent in the bound, is positive; while it decays to zero when $\Psi_{net}\left(k,n,N;d,\epsilon\right)<0$. This is why $\rho^{exp}(\delta;d,\epsilon)$ is defined to satisfy $\Psi_{net}\left(k,n,N;d,\epsilon\right)=0$ in (4.11), so that for any $\rho$ slightly less than $\rho^{exp}(\delta;d,\epsilon)$ we will have $\Psi_{net}\left(k,n,N;d,\epsilon\right)<0$ and hence the bound decay to zero.

Precisely, we just need $k/n\to\rho<(1-\gamma)\rho^{exp}(\delta;d,\epsilon)$ for small $\gamma>0$. In this regime of $\rho<(1-\gamma)\rho^{exp}(\delta;d,\epsilon)$ we have $\text{Prob}\left(\|Ax\|_1\leq(1-2\epsilon)d\|x\|_1\right)\to 0$. This means therefore, $\text{Prob}\left(\|Ax\|_1\geq(1-2\epsilon)d\|x\|_1\right)\to 1$ as the problem size $(k,n,N)\to\infty$, $n/N\to\delta\in(0,1)$ and $k/n\to\rho$, at a rate exponential in $n$.

### Corollary 4.3.2

The first part of this proof uses ideas from the proof of Proposition 4.3.1 which is the same as Theorem 16 in [14]. We consider a bipartite graph $G(U,V,E)$ with $|U|=N$ left vertices, $|V|=n$ right vertices and left degree $d$. For a fixed $S\subset U$ where $|S|=s\leq k$, $G$ fails to be an expander on $S$ if $|\Gamma(S)| < (1-\epsilon)ds$. This means that in a sequence of $ds$ vertex indices at least $\epsilon ds$ of the these indices are in the collision set that is identical to some preceding value in the sequence.

Therefore, the probability that a neighbour chosen uniformly at random is in the collision set is at most $ds/n$ and, treating each event independently, then the probability that a set of $\epsilon ds$ neighbours chosen at random are in the collision set is at most $(ds/n)^{\epsilon ds}$. There are $\binom{ds}{\epsilon ds}$ ways of choosing a set of $\epsilon ds$ points from a set of $ds$ points and $\binom{N}{s}$ ways of choosing each set $S$ from $U$. This means therefore that the probability that $G$ fails to expand in at least one of the sets $S$ of fixed size $s$ can be bounded above by a union bound

$$\text{Prob}\left(G \text{ fails to expand on } S\right) \leq \binom{N}{s}\binom{ds}{\epsilon ds}\left(\frac{ds}{n}\right)^{\epsilon ds}. \tag{4.180}$$

We define $p_s$ to be the right hand side of (4.180) and we use the right hand side of the Stirling's inequality (2.11) to upper bound $p_s$ as thus

$$\begin{aligned} p_s < \frac{5}{4}\left[2\pi\frac{\epsilon ds}{ds}\left(1-\frac{\epsilon ds}{ds}\right)\epsilon ds\right]^{-\frac{1}{2}} \exp\left[ds\mathrm{H}\left(\frac{\epsilon ds}{ds}\right)\right] \\ \times\frac{5}{4}\left[2\pi\frac{s}{N}(1-\frac{s}{N})N\right]^{-\frac{1}{2}} \exp\left[N\mathrm{H}\left(\frac{s}{N}\right)\right] \times \left(\frac{ds}{n}\right)^{\epsilon ds} \end{aligned} \tag{4.181}$$

Writing the last multiplicand in exponential form and simplifying makes (4.181) become

$$p_s < p_{max}(N,s;d,\epsilon)\cdot\exp\left[N\cdot\Psi\left(s,n,N;d,\epsilon\right)\right], \tag{4.182}$$

where

$$\Psi\left(s,n,N;d,\epsilon\right) = \mathrm{H}\left(\frac{s}{N}\right) + \frac{ds}{N}\mathrm{H}\left(\epsilon\right) + \frac{\epsilon ds}{N}\log\left(\frac{ds}{n}\right) \tag{4.183}$$

$$p_{max}(N,s;d,\epsilon) = \left(\frac{5}{4}\right)^2\cdot\frac{1}{2\pi s}\cdot\left[\frac{N}{\epsilon(1-\epsilon)(N-s)d}\right]^{\frac{1}{2}} \tag{4.184}$$

is a polynomial in $N$ and $s$ for each $d$ and $\epsilon$ fixed. Finally $G$ fails to be an expander if it fails to expand on at least one set $S$ of any size $s \leq k$. This means therefore that

$$\text{Prob}\left(G \text{ fails to be an expander}\right) \leq \sum_{s=1}^{k} p_s. \tag{4.185}$$

From (4.182) we have

$$\begin{aligned} \sum_{s=2}^{k} p_s &< \sum_{s=2}^{k} p_{max}(N,s;d,\epsilon)\cdot\exp\left[N\cdot\Psi\left(s,n,N;d,\epsilon\right)\right] && (4.186) \\ &< p'_{max}(N,k;d,\epsilon)\cdot\exp\left[N\cdot\Psi\left(k,n,N;d,\epsilon\right)\right], && (4.187) \end{aligned}$$

where $p'_{max}(N,k;d,\epsilon) = k \cdot p_{max}(N,k;d,\epsilon)$ and we achieved the bound from (4.186) to (4.187) by upper bounding the sum with the product of the largest term in the sum (which is when $s=k$ since $k<N/2$) and one plus the number of terms in the sum, giving $k$. Hence from (4.185) and (4.187) we have

$$\text{Prob}\left(G \text{ fails to be an expander}\right) < p'_{max}(N,k;d,\epsilon) \cdot \exp\left[N \cdot \Psi\left(k,n,N;d,\epsilon\right)\right]. \qquad (4.188)$$

As the problem size, $(k,n,N)$, grows the exponential term will be driving the probability in (4.188), hence having

$$\Psi\left(k,n,N;d,\epsilon\right) < 0 \qquad (4.189)$$

yields $\text{Prob}\left(G \text{ fails to be an expander}\right) \rightarrow 0$ as $(k,n,N) \rightarrow \infty$.

Now let $k/n \rightarrow \rho \in (0,1)$ and $n/N \rightarrow \delta \in (0,1)$ as $(k,n,N) \rightarrow \infty$ and we define $\rho_{bi}^{exp}\left(\delta;d,\epsilon\right)$ as the limiting value of $k/n$ that satisfies $\Psi\left(k,n,N;d,\epsilon\right) = 0$ for each fixed $\epsilon$ and $d$ and all $\delta$. Note that for fixed $\epsilon$, $d$ and $\delta$ it is deducible from our analysis of $\psi_n(\cdot)$ in Section 4.3.2 that $\Psi\left(k,n,N;d,\epsilon\right)$ is a strictly monotonically increasing function of $k/n$. Therefore for any $\rho < \rho_{bi}^{exp}\left(\delta;d,\epsilon\right)$, $\Psi\left(k,n,N;d,\epsilon\right) < 0$ as $(k,n,N) \rightarrow \infty$, $\text{Prob}\left(G \text{ fails to be an expander}\right) \rightarrow 0$ and $G$ becomes an expander with probability approaching one exponentially in $N$ which is the same as exponential growth in $n$ since $n \rightarrow N\rho$.

# Chapter 5

# Conclusions

## 5.1 Summary

### Chapter One

In this chapter we showed that this work is centred around a fundamental linear algebra question of solving an underdetermined linear system. This naturally involves the question of uniqueness of the solution out of the infinitely many solutions to the system. In addition, computationally, there is a further question on the accuracy of a numerical solution which is dependent on the stability and convergence of the numerical algorithm used. However, in the target applications of this work a parsimonious (sparse) solution is sought after which guarantees uniqueness. A further restriction on the rectangular matrix, say $A$, of the underdetermined system guarantees accuracy in the form of either exact recovery or a bound on the reconstruction error. One of the restrictions on $A$ is that it has small enough restricted isometry constants (RIC). This requirement of small enough RIC of $A$ is equivalent to bounded condition numbers of submatrices of $A$ with number of columns of the order of sparsity of the solution. There are combinatorially many of these submatrices hence RIC analysis is similar to classical eigen-analysis except for its combinatorial nature.

Precisely, the lower and upper RIC of a matrix tell us by how much the matrix scales the length of a given $k$-sparse vector. If the length is measured in the $\ell_2$-norm we have RIC$_2$ while if the length is measured in the $\ell_1$-norm we have RIC$_1$. In Section 1.1.1 we defined RIC$_2$ as the largest and smallest deviation from unity of the eigenvalues of the Gram matrix of submatrices with $k$ columns. Current research on RIC$_2$ has been sparked by compressed sensing but its use has spread into other areas including sparse approximation and approximation theory. Its relation to $n$-widths has been established and with new extensions of compressed sensing like matrix completion it has been use as a tool of analysis in this area too. There are matrices whose

$\mathrm{RIC}_2$ is not sufficiently small for the desired application but some of these have sufficiently small $\mathrm{RIC}_1$. This class includes adjacency matrices of lossless expander graphs, theme of Section 1.1.2.

Interestingly, the focus of research in these two type of RICs are different. Researchers on $\mathrm{RIC}_2$ have not been successful so far in designing deterministic matrices that have small $\mathrm{RIC}_2$ but are able to show that random matrices have small $\mathrm{RIC}_2$ with optimal $n$. One of the main issues is how to compute the $\mathrm{RIC}_2$ of these random ensembles. While in the case $\mathrm{RIC}_1$, its computation is trivial but even the probabilistic construction of the class of matrices that have small $\mathrm{RIC}_1$ is far from trivial to implement for the practitioner. This is why the first part of this work concentrated on the computation of $\mathrm{RIC}_2$ while the second part concentrated on the probabilistic construction of matrices that have small $\mathrm{RIC}_1$.

The relationship of $\mathrm{RIC}_2$ to classical eigen-analysis warranted a review of some of the classical literature on the spectrum of random matrices, particularly the Gaussian and Wishart ensembles. This review included a discussion on the universality principle of random matrices and a discussion on extreme eigenvalues of Wishart matrices in Section 1.2. The universality principle lends support to our claim that the $\mathrm{RIC}_2$ of the Gaussian ensembles can be a model for all other random ensembles. This is manifested by some of the theorems, lemmas and propositions about the distribution of the extreme eigenvalues of a Wishart matrix. In Section 1.3 we briefly discussed expander graphs and their adjacency matrices that have small $\mathrm{RIC}_1$ of optimal order. Expander graphs have a good expansion that makes them of interest to many application areas including communication networks, coding theory, statistical mechanics, pure mathematics, etc. Their explicit construction with optimal parameters is still an open problem but optimal probabilistic constructions are possible.

Our study of restricted isometry constants is motivated by compressed sensing, hence Section 1.4. In compressed sensing we are interested on the effect of the application of a matrix to a *simple* vector. The simplicity of the vector could be sparsity or compressibility. The compressed sensing problem is essentially trying to solve an underdetermined linear system by exploiting the fact that the solution has this in-built simplicity. The RICs are part of the tools used in compressed sensing to guarantee that the solution recovered is exact or closely approximates the original vector with a small error in some norm. The two main tasks in compressed sensing is the design of sensing matrices and algorithms.

Good sensing matrices are those that have number of rows $n$ scaling linearly with the simplicity of the vector where the dimension of the vector only has a minor logarithmic effect. The compressed sensing problem is posed as an $\ell_0$-minimization problem which is intractable but can be relaxed into an $\ell_1$-minimization which can be solved with several algorithms. Algorithms have also been designed to tackle the $\ell_0$-minimization problem by doing a greedy search and they include Iterative Hard Thresholding (IHT), Orthogonal Matching Pursuit (OMP) and Compressive Sampling Matching Pursuits (CoSAMP) for dense matrices and Sequential Sparse Matching Pursuit (SSMP) and Expander Recovery (ER) for sparse binary matrices.

**Chapter Two**

We focused on the computation of RIC$_2$ but this is NP-hard since one has to consider all $\binom{N}{k}$ submatrices composed of $k$ columns. However, it is possible to derive asymptotic bounds of RIC$_2$. The bounds we talk about here are all derived in the so called *proportional growth asymptotics* framework where $k/n \to \rho \in (0,1)$ and $n/N \to \delta \in (0,1)$ as the problem size $(k,n,N) \to \infty$ when we have an $n \times N$ matrix and we look for a $k$-sparse solution.

The first set of bounds were done by Candès and Tao [39] using concentration of measure inequalities for the singular values of Gaussian matrices and using a union bound over all $\binom{N}{k}$ possible submatrices of $k$ columns. We showed these bounds and their plots in Section 2.2. It can be seen from the plots how loose these bounds were, the lower RIC$_2$ quickly goes to 1 as the ratio $k/n$ increase. At 1 and beyond the bounds are meaningless. The second set of bounds which were a significant improvement on the Candès and Tao bounds were done by Blanchard, Carits and Tanner [19]. They used more accurate bounds on the probability density function of extreme eigenvalues of Wishart matrices due to Edelman [62]. Employing large deviation analysis, they also used a union bound. The bounds and their plots are given in Section 2.2.

In both prior bounds the union bound was used, this treats all the $\binom{N}{k}$ column submatrices as independent, implying independence in their extreme singular values. In a departure from this assumption we assumed that submatrices with significant overlap may not have independent extreme singular values. We still used the probability density functions bounds as used by Blanchard et al but used a grouping technique to group all submatrices with significant column overlap into groups and used a probabilistic argument to quantify the number of groups sufficient to cover all the $\binom{N}{k}$ subsets of $[N]$ that are of size $k$. This greatly reduced the combinatorial term, $\binom{N}{k}$, and hence the improvement on the prior bounds.

In Section 2.3, we presented our bounds and their plots which we followed with a discussion on their derivation. We also showed how our bounds compared to empirically derived lower bounds of RIC$_2$ computable from algorithms due to [83] and [60]. In addition, a comparison of our bounds to those of Blanchard et al was also given. In the discussion that followed in this section, we stated and proved the covering lemma, which give guarantees to our covering argument. Both the grouping scheme and the covering argument are new innovations in such works. In Section 2.4 we showed that even though our bounds were derived in an asymptotic setting, they are valid for finite cases of the problem size $(k,n,N)$.

Section 2.5 discussed the implications of our results to compressed sensing. Blanchard et al in [20] use their RIC$_2$ bounds to compare performance guarantees of compressed sensing algorithms in a phase transition framework. Our bounds were a significant improvement on the Blanchard et al bounds particularly the upper RIC$_2$ bound. However, the phase transition using our bounds did not improve much those of Blanchard et al [20]. The main reason is that, it is the lower RIC$_2$ that drives the phase transitions and the bound on this by Blanchard et al was already very tight with ours being only a meagre improvement on theirs for the lower $\mathrm{RIC}_2$. To put things in proper perspective we briefly discussed a select compressed sensing algorithms whose phase transitions we compared.

We concluded the chapter with the proof of the main theorem of our bounds. This proof is similar to that of Blanchard et al in [19] but we adjusted it where necessary to clearly compute the constants because we needed them for the computation of the finite $N$ probabilities to demonstrate the validity of our bounds for finite problem sizes.

**Chapter Three**

One disadvantage of the bounds we derived in Chapter 2 is that they are not given explicitly but are hidden in a set of equations that has to be solve whenever one wants to compute these bounds. In this chapter we tried to simplify the bounds. We analysed three different regimes of $\rho$ and $\delta$. In the first case we fix $\delta$ and consider $\rho$ very small, $\rho \ll 1$; the second case considered a fixed $\rho$ and very small $\delta$, $\delta \ll 1$; and the third case is where we consider both $\delta$ and $\rho$ small and going to zero but $\rho$ going to zero at a rate inverse logarithmic to the reciprocal of $\delta$ along a path $\gamma$. Based on the third case we derived functions of $\gamma$ which the bounds converge to independently of $\delta$ and $\rho$. Analysis of these bounds in the regime of $\delta$ and $\rho$ considered will be greatly simplified if one uses these simple functions of $\gamma$ that the bounds converge to.

In Section 3.3 we showed how one can use these formulae to approximate the order constant in the optimal number of measurement, $n \geq Ck \log(N/k)$, for the selected compressed sensing algorithms discussed in Chapter 2 and the order constant $C$ is given by $\gamma$. Amazingly, the values we get are very tight compared to what is known. Similarly, from these formulae we derive approximations of $n$ for Orthogonal Matching Pursuit (OMP) which is known to be sub-optimal. In Section 3.4 we demonstrate the accuracy of these formulae by showing plots of relative errors between these formulae and the Blanchard et al bounds. We used the Blanchard et al bounds because in these types of values of $\delta$ and $\rho$ they are easier to compute than our bounds and the fact is, in these regime of $\delta$ and $\rho$, our bounds match those of Blanchard et al.

We conclude the chapter by giving the proofs of the main compressed sensing corollaries and then the proofs of the main theorems of the formulae. For the proof of the main theorems, in all cases we use the same strategy. We know that the tail probability of the $\mathrm{RIC}_2$ is bounded by a product of a polynomial and an exponential and that the exponential derives the bound. When its large deviation exponent is negative the bound goes to zero as the problem size grows. Our bounds are lower bounds that make this exponent negative. Any bound from above these bounds is also going to make the exponent negative but any bound below these will make the exponent positive in which case the bound on the tail probability will not be meaningful.

**Chapter Four**

In this Chapter the concentration is on the probabilistic construction of sparse sensing matrices that are non-mean zero with fixed number of nonzero entries in each column. These matrices have a one-to-one correspondence with lossless expander graphs. More precisely, we derive bounds on the tail probability of the cardinality of the *set of neighbours*, which is the number of rows with at least one nonzero element. Deducible from this is a bound on the expansion of the graphs that underlay these matrices. The expansion is of interest to other applications different from compressed sensing. Furthermore, from this bound and RIC$_1$ we derive corollaries that are sampling theorems for the existence of expander graphs or the matrices we consider and sampling theorems for compressed sensing algorithms. We also compared quantitatively, performance guarantees of compressed sensing algorithms designed for the matrices we considered and made a quantitative comparison of $\ell_1$-minimization performance guarantees for dense mean zero Gaussian with the sparse non-mean zero matrices we considered in this chapter.

The derivation of the tail bound on the probability of the cardinality of the set of neighbours used a novel technique of *dyadic set splitting*. In Section 4.2.2 we discussed RIC$_1$ and its implications to compressed sensing and expander graphs particularly in its use to derive sampling theorems for compressed sensing measurement matrices and the existence of expander graphs. We discussed our results and their derivation in Section 4.3 where we presented numerical plots that support our results. The second half of this section set the stage for the proof of the main theorem. Here we presented lemmas, corollaries and propositions (and their proofs) that we used to prove Theorem 4.2.4.

In Section 4.4 we investigate the implications of our results for compressed sensing algorithms. We derived quantitative performance guarantees based on RIC$_1$. The latter is done for $\ell_1$-minimization and the greedy algorithms: Expander Matching Pursuit (EMP), Sparse Matching Pursuit (SMP), Sequential Sparse Matching Pursuit (SSMP), Left Degree Dependent Signal Recovery (LDDSR) and Expander Recovery (ER). The phase transition region for ER (also for LDDSR) is higher than the one for $\ell_1$-minimization which in turn is higher than that of SSMP (also of SMP and EMP). Furthermore, we computed phase transitions comparing $\ell_1$-minimization for dense and sparse matrices, which show that a higher phase transition for sparse matrices than dense matrices.

In Section 4.5 we did all the remaining proofs. First we showed that Theorem 4.2.4 holds for small sparsity, $s$, with $s = 2,\ 3$ and 8. Then we proceeded with the proof for large $s$. The key tool in this proof is the splitting lemma presented in Section 4.3. Then we proved the second theorem part of whose proof was given in [15]. We therefore, only do the second case of the theorem when the nonzeros of the matrices take on random signs. In the rest of this section we did the proofs of the main corollaries in the chapter.

## 5.2 Possible Extensions

**The $\ell_2$-norm Restricted Isometry Constant Bounds**

Application wise, especially in compressed sensing, there seems to be a consensus that analysis using $\mathrm{RIC}_2$ bounds gives results that are far away from what obtains in practice and hence it seems pointless to improve on our bounds. However, one can still argue that this analysis is important because it gives us the worst-case scenario and mathematically, further investigation into how small these bounds are will tell us about extreme singular values of submatrices. It is in this regard that we suggest below some possible extensions of this work.

- Generic chaining arguments has been used by Mendelson et al in [104] to prove RIP-2 (they referred to it in their paper as the uniform uncertainty principle) for subgaussian matrix ensembles. These chaining arguments are yet to be employed to derive quantitative $\mathrm{RIC}_2$ bounds. There is a chance that such arguments can be used to derive smaller bounds than ours. For the most recent survey of generic chaining the reader is referred to [134].

- One could also potentially employ *Small Value Probability* to improve on the bound on the smallest eigenvalue and hence the lower $\mathrm{RIC}_2$ bound. Small value probabilities or small deviations study the decay probability of positive random variables have near zero. Theoretically, the large deviation analysis we used in our derivation gives a loose bound on the smallest eigenvalue. However, our results and the previous results of Blanchard et al show that the lower bound is already very close to the observed empirical lower bounds, so is any little gain worth the effort? For details on small value probability see lecture notes [93] and the website devoted to this subject [101].

- We stated that $\mathrm{RIC}_2$ analysis give results that are far from what is observed in practice. Therefore, a possible extension is to move away from this worse-case analysis to average-case analysis. This could be achieved by using *smoothing* techniques as used in the study of condition numbers, see [29] and the references therein.

- Furthermore, the recent extension of compressed sensing, matrix completion, also uses $\mathrm{RIC}_2$ of the linear map to guarantee recovery of low rank matrix. The equivalence of RIP-2 has been derived for matrix completion [118]. However, since the $\mathrm{RIC}_2$ cannot be computed, one could derive computable bounds for these $\mathrm{RIC}_2$, similar to what we did and possibly employing some of the methods we used.

- For the asymptotic formulae for the bounds, it would be interesting to do similar formulae using our bounds instead of the BCT bounds. Other possible improvements for the asymptotic expansion of the bounds depend on the bound on the tail probability which is derived from the derivation of the bounds. With another improvement on the bounds where the bound on the tail probabilities is given or is deducible, one can use that to improve the asymptotic formulae.

**Sparse matrices with the $\ell_1$-norm Restricted Isometry Constants**

The derivation of tail bounds, quantitative sampling theorems and the comparison of performance guarantees of compressed sensing algorithms in Chapter 4 are all prototypes. Consequently, there are several possible extensions of this work. We suggest some of these possible extensions in the following paragraphs.

- Firstly, possibly there are other methods of deriving similar or better bounds on the tail probability of the cardinality of the set of neighbours. Even within our derivation there is room for improvement. The bound on the polynomial term resulting from the Stirling inequality bound on the combinatorial terms can be improved. Improving the bound on the polynomial term may result in a smaller bound.

- Secondly, in the phase transition comparison of the performance of compressed sensing algorithms we were only able to compute the phase transitions curves for finite $n$. This is because the large deviation exponent, $\Psi\left(a_s,\ldots,a_2,d\right)$ in (4.3), in the tail bound can only be computed for finite $n$. It would be interesting to investigate the asymptotic behaviour of this exponent and hence derive phase transition curves in the proportional growth asymptotics.

- Again in the phase transition comparison of compressed sensing algorithms we used the method of Blanchard et al, in [20], of computing the phase transition curves in the $(k/n, n/N)$ plane. In the case of the matrices considered in this work, we have an extra dependence on the degree $d$ of the $(k,d,\epsilon)$-expander graph. One possible way of properly capturing this dependence maybe to derive the phase transition in the $((dk)/n, n/N)$ plane. This might simplify the asymptotics of the large deviation exponent suggested in the preceding paragraph.

- We have mentioned in Section 4.4.2 that numerical simulation has shown a comparable average performance of SSMP and SMP to $\ell_1$-minimization for SE matrices and a comparable average performance of $\ell_1$-minimization for sparse SE matrices to dense Gaussian random matrices. A natural extension therefore is to do the same for SSE matrices and then extend this to ER and LDDSR algorithms.

- From a graph theorist point of view regular graphs are harder object than their irregular counterparts and there are applications that are more interested on the irregular case. It might be more useful to such applications to do similar tail bounds for expander graphs that are irregular. One easy way of doing this is to take the minimum degree of these graphs to be $d$ and to lower bound all the other degrees by $d$. This would reproduce our results for the fixed $d$ case. One could potentially get a smaller tail bound than this if one uses the distribution of the degrees of the irregular graph.

- Closely, related to the above is a similar question about expander graphs that have a tree structure in the set of left nodes. In this case the graphs can be either regular or irregular. It would be interesting to investigate the possibility of doing similar bounds for such graphs.

- Recently, Khajehnejad et al in [87] proposed operators they called *subspace expanders* and an algorithm for matrix rank minimization. These subspace expanders, quoting the authors [87] are "inspired by the well known expander graphs based measurement matrices in compressed sensing". Potentially, one may be able to use our tail bounds or the method of *dyadic set splitting* to improve upon the theoretical guarantees they gave in [87].

- In addition, one could conduct both worse-case and average-case comparisons of performance guarantees of some of the proposed algorithms for matrix completion and rank minimization through the phase transition framework.

- Generally, the explicit construction of expander graphs is still an open problem, one could explore the use of similar idea to the *dyadic splitting* to be combined with existing sub-optimal explicit construction methods to make an improvement in these constructions.

# Bibliography

[1] Abramowitz, M., and Stegun, I. *Handbook of mathematical functions.* Dover publications, 1964.

[2] Alon, N. Eigenvalues and expanders. *Combinatorica 6*, 2 (1986), 83–96.

[3] Alon, N., and Milman, V. Eigenvalues, expanders and superconcentrators. In *Proceedings of the 25th Annual Symposium on Foundations of Computer Science* (1984), pp. 320–322.

[4] Arora, S., Leighton, T., and Maggs, B. On-line algorithms for path selection in a nonblocking network. In *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing* (1990), ACM, pp. 149–158.

[5] Babacan, S., Molina, R., and Katsaggelos, A. Bayesian compressive sensing using laplace priors. *IEEE Transactions on Image Processing 19*, 1 (2010), 53–63.

[6] Bah, B., and Tanner, J. Improved bounds on restricted isometry constants for gaussian matrices. *SIAM Journal on Matrix Analysis and Applications 31*, 5 (2010), 2882–2898.

[7] Bah, B., and Tanner, J. Bounds of restricted isometry constants in extreme asymptotics: formulae for gaussian matrices. *Arxiv preprint arXiv:1207.4883* (2012).

[8] Bah, B., and Tanner, J. Vanishingly sparse matrices and expander graphs, with application to compressed sensing. *Arxiv preprint arXiv:1207.3094* (2012).

[9] Bajwa, W., Haupt, J., Raz, G., Wright, S., and Nowak, R. Toeplitz-structured compressed sensing matrices. In *Proceedings of the IEEE/SP 14th Workshop on Statistical Signal Processing, 2007. SSP'07.* (2007), IEEE, pp. 294–298.

[10] Baraniuk, R. Compressive sensing [lecture notes]. *IEEE Signal Processing Magazine 24*, 4 (2007), 118–121.

[11] Baraniuk, R. More is less: Signal processing and the data deluge. *Science 331*, 6018 (2011), 717.

[12] Baraniuk, R., Davenport, M., DeVore, R., and Wakin, M. A simple proof of the restricted isometry property for random matrices. *Constructive Approximation 28*, 3 (2008), 253–263.

[13] Bassalygo, L., and Pinsker, M. Complexity of an optimum nonblocking switching network without reconnections. *Problemy Peredachi Informatsii 9*, 1 (1973), 84–87.

[14] Berinde, R. Advances in sparse signal recovery methods. Master's thesis, Massachusetts Institute of Technology, 2009.

[15] Berinde, R., Gilbert, A., Indyk, P., Karloff, H., and Strauss, M. Combining geometry and combinatorics: A unified approach to sparse signal recovery. In *Proceedings of the 46th Annual Allerton Conference on Communication, Control, and Computing, 2008.* (2008), IEEE, pp. 798–805.

[16] Berinde, R., and Indyk, P. Sparse recovery using sparse random matrices. *preprint* (2008).

[17] Berinde, R., and Indyk, P. Sequential sparse matching pursuit. In *Proceedings of the 47th Annual Allerton Conference on Communication, Control, and Computing, 2009. Allerton 2009.* (2009), IEEE, pp. 36–43.

[18] Berinde, R., Indyk, P., and Ruzic, M. Practical near-optimal sparse recovery in the $l_1$ norm. In *Proceedings of the 46th Annual Allerton Conference on Communication, Control, and Computing, 2008.* (2008), IEEE, pp. 198–205.

[19] Blanchard, J., Cartis, C., and Tanner, J. Compressed sensing: How sharp is the restricted isometry property? *SIAM Review 53*, 1 (2011), 105–125.

[20] Blanchard, J., Cartis, C., Tanner, J., and Thompson, A. Phase transitions for greedy sparse approximation algorithms. *Applied and Computational Harmonic Analysis 30*, 2 (2011), 188–203.

[21] Blanchard, J., and Tanner, J. GPU accelerated greedy algorithms for compressed sensing. *Preprint* (2012).

[22] Blanchard, J., and Thompson, A. On support sizes of restricted isometry constants. *Applied and Computational Harmonic Analysis 29*, 3 (2010), 382–390.

[23] Blanchard, J. D., Cartis, C., and Tanner, J. Decay properties for restricted isometry constants. *IEEE Signal Processing Letters 16*, 7 (2009), 572–575.

[24] Blumensath, T., and Davies, M. Normalized iterative hard thresholding: Guaranteed stability and performance. *IEEE Journal of Selected Topics in Signal Processing 4*, 2 (2010), 298–309.

[25] Blumensath, T., and Davies, M. E. Iterative hard thresholding for compressed sensing. *Applied and Computational Harmonic Analysis* (April 2009).

[26] Broder, A., Frieze, A., and Upfal, E. Static and dynamic path selection on expander graphs (preliminary version): a random walk approach. In *Proceedings of the 29th Annual ACM Symposium on Theory of Computing* (1997), ACM, pp. 531–539.

[27] Bruckstein, A., Donoho, D., and Elad, M. From sparse solutions of systems of equations to sparse modeling of signals and images. *SIAM Review 51*, 1 (2009), 34.

[28] Buhrman, H., Miltersen, P., Radhakrishnan, J., and Venkatesh, S. Are bitvectors optimal? In *Proceedings of the 32nd Annual ACM Symposium on Theory of Computing* (2000), ACM, pp. 449–458.

[29] Bürgisser, P., Cucker, F., and Lotz, M. General formulas for the smoothed analysis of condition numbers. *Comptes Rendus Mathematique 343*, 2 (2006), 145–150.

[30] Calderbank, R., Jafarpour, S., and Schapire, R. Compressed learning: Universal sparse dimensionality reduction and learning in the measurement domain. *Manuscript* (2009).

[31] Candès, E., and Recht, B. Exact matrix completion via convex optimization. *Foundations of Computational Mathematics 9*, 6 (2009), 717–772.

[32] Candes, E., Romberg, J., and Tao, T. Stable signal recovery from incomplete and inaccurate measurements. *Communications on Pure and Applied mathematics 59*, 8 (2006), 1207–1223.

[33] Candès, E., and Tao, T. Near-optimal signal recovery from random projections: universal encoding strategies? *IEEE Transactions on Information Theory 52* (December 2006), 5406–5425.

[34] Candes, E., and Tao, T. The dantzig selector: statistical estimation when $p$ is much larger than $n$. *The Annals of Statistics 35*, 6 (2007), 2313–2351.

[35] Candes, E., and Tao, T. The power of convex relaxation: Near-optimal matrix completion. *IEEE Transactions on Information Theory 56*, 5 (2010), 2053–2080.

[36] Candès, E., and Wakin, M. An introduction to compressive sampling. *IEEE Signal Processing Magazine 25*, 2 (2008), 21–30.

[37] Candès, E. J. The restricted isometry property and its implications for compressed sensing. *Comptes Rendus de l'Académie des Sciences, Paris 346*, 9–10 (2008), 589–592.

[38] Candès, E. J., Romberg, J., and Tao, T. Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information. *IEEE Transactions on Information Theory 52*, 2 (2006), 489–509.

[39] Candès, E. J., and Tao, T. Decoding by linear programming. *IEEE Transactions on Information Theory 51*, 12 (2005), 4203–4215.

[40] Capalbo, M. Explicit constant-degree unique-neighbor expanders, 2001.

[41] Capalbo, M., Reingold, O., Vadhan, S., and Wigderson, A. Randomness conductors and constant-degree lossless expanders. In *Proceedings of the 34th annual ACM symposium on Theory of computing* (2002), ACM, pp. 659–668.

[42] Cevher, V. Learning with compressible priors. *NIPS, Vancouver, BC, Canada* (2008), 7–12.

[43] Cevher, V., Duarte, M., Hegde, C., and Baraniuk, R. Sparse signal recovery using markov random fields. In *Proceedings of Workshop on Neural Information Processing Systems (NIPS)* (2008), Citeseer.

[44] Chandar, V. A negative result concerning explicit matrices with the restricted isometry property. *preprint* (2008).

[45] Chen, W., Rodrigues, M., and Wassell, I. On the use of unit-norm tight frames to improve the average mse performance in compressive sensing applications. *IEEE Signal Processing Letters*, 99 (2012), 1–1.

[46] Chen, Z., and Dongarra, J. Condition numbers of gaussian random matrices. *Arxiv preprint arXiv:0810.0800* (2008).

[47] Cohen, A. *Numerical analysis of wavelet methods*, vol. 32. JAI Press, 2003.

[48] Cohen, A., Dahmen, W., and DeVore, R. Compressed sensing and best $k$-term approximation. *Journal of American Mathematical Society 22*, 1 (2009), 211–231.

[49] Cormode, G., and Muthukrishnan, S. Combinatorial algorithms for compressed sensing. *Structural Information and Communication Complexity* (2006), 280–294.

[50] Dai, W., and Milenkovic, O. Subspace pursuit for compressive sensing signal reconstruction. *IEEE Transactions on Information Theory 55*, 5 (2009), 2230–2249.

[51] d'Aspremont, A., Bach, F., and Ghaoui, L. Optimal solutions for sparse principal component analysis. *Journal of Machine Learning Research 9* (2008), 1269–1294.

[52] d'Aspremont, A., Bach, F., and Ghaoui, L. Optimal solutions for sparse principal component analysis. *Journal of Machine Learning Research 9* (2008), 1269–1294.

[53] Davenport, M., Wakin, M., and Baraniuk, R. Detection and estimation with compressive measurements. *Dept. of ECE, Rice University, Technical Report* (2006).

[54] Demmel, J. *Numerical linear algebra*, vol. 1. Center for Pure and Applied Mathematics, Dept. of Mathematics, University of California, 1993.

[55] DeVore, R. Deterministic constructions of compressed sensing matrices. *Journal of Complexity 23*, 4-6 (2007), 918–925.

[56] Donoho, D. *Neighborly polytopes and sparse solution of underdetermined linear equations.* Citeseer, 2005.

[57] Donoho, D., and Tanner, J. Counting faces of randomly-projected polytopes when the projection radically lowers dimension. *American Mathematical Society 22*, 1 (2009), 1–53.

[58] Donoho, D., Vetterli, M., DeVore, R., and Daubechies, I. Data compression and harmonic analysis. *IEEE Transactions on Information Theory 44*, 6 (1998), 2435–2476.

[59] Donoho, D. L. Compressed sensing. *IEEE Transactions on Information Theory 52*, 4 (2006), 1289–1306.

[60] Dossal, C., Peyré, G., and Fadili, J. A numerical exploration of compressed sampling recovery. *Linear Algebra and its Applications 432*, 7 (2010), 1663–1679.

[61] Dyson, F. The threefold way. algebraic structure of symmetry groups and ensembles in quantum mechanics. *Journal of Mathematical Physics 3*, 1199 (1962).

[62] Edelman, A. Eigenvalues and condition numbers of random matrices. *SIAM Journal on Matrix Analysis and Applications 9* (1988), 543–560.

[63] Edelman, A. *Eigenvalues and condition numbers of random matrices.* PhD thesis, Massachusetts Institute of Technology, 1989.

[64] Edelman, A., and Rao, N. R. Random matrix theory. *Acta Numerica 14* (2005), 233–297.

[65] Elad, M. Optimized projections for compressed sensing. *IEEE Transactions on Signal Processing 55*, 12 (2007), 5695–5702.

[66] Fornasier, M. *Theoretical foundations and numerical methods for sparse recovery*, vol. 9. Walter de Gruyter, 2010.

[67] Foucart, S. A note on guaranteed sparse recovery via $l_1$-minimization. *Applied and Computational Harmonic Analysis 29*, 1 (2010), 97–103.

[68] Foucart, S., and Lai, M.-J. Sparsest solutions of underdetermined linear systems via $\ell_q$-minimization for $0 < q \leq 1$. *Applied and Computational Harmonic Analysis 26*, 3 (2009), 395–407.

[69] Garnaev, A., and Gluskin, E. The widths of a euclidean ball. In *Doklady Akademii Nauk SSSR* (1984), vol. 277, pp. 1048–1052.

[70] Geman, S. A limit theorem for the norm of random matrices. *The Annals of Probability 8*, 2 (1980), 252–261.

[71] Girko, V., and Girko, V. *An introduction to statistical analysis of random arrays.* Vsp, 1998.

[72] Guruswami, V., Umans, C., and Vadhan, S. Unbalanced expanders and randomness extractors from parvaresh-vardy codes. In *Proceedings of the 22nd Annual IEEE Conference on Computational Complexity, 2007. CCC'07.* (2007), IEEE, pp. 96–108.

[73] Haupt, J., Bajwa, W., Raz, G., and Nowak, R. Toeplitz compressed sensing matrices with applications to sparse channel estimation. *IEEE Transactions on Information Theory 56*, 11 (2010), 5862–5875.

[74] Haupt, J., and Nowak, R. Compressive sampling for signal detection. In *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing, 2007, ICASSP 2007.* (2007), vol. 3, IEEE, pp. III–1509.

[75] Herman, M., and Strohmer, T. High-resolution radar via compressed sensing. *IEEE Transactions on Signal Processing 57*, 6 (2009), 2275–2284.

[76] Hoory, S., Linial, N., and Wigderson, A. Expander graphs and their applications. *Bulletin of the American Mathematical Society 43*, 4 (2006), 439–562.

[77] Horn, R., and Johnson, C. *Matrix analysis*. Cambridge University Press, 1990.

[78] Indyk, P., and Ruzic, M. Near-optimal sparse recovery in the $\ell_1$-norm. In *Proceedings of the 49th Annual IEEE Symposium on Foundations of Computer Science, 2008. FOCS'08.* (2008), IEEE, pp. 199–207.

[79] Jafarpour, S., Xu, W., Hassibi, B., and Calderbank, R. Efficient and robust compressed sensing using high-quality expander graphs. *Arxiv preprint arXiv:0806.3802* (2008).

[80] Jafarpour, S., Xu, W., Hassibi, B., and Calderbank, R. Efficient and robust compressed sensing using optimized expander graphs. *IEEE Transactions on Information Theory 55*, 9 (2009), 4299–4308.

[81] James, A. Distributions of matrix variates and latent roots derived from normal samples. *The Annals of Mathematical Statistics* (1964), 475–501.

[82] Johnson, W., and Lindenstrauss, J. Extensions of lipschitz mappings into a hilbert space. *Contemporary Mathematics 26*, 189-206 (1984), 1–1.

[83] Journée, M., Nesterov, Y., Richtárik, P., and Sepulchre, R. Generalized power method for sparse principal component analysis. *Journal of Machine Learning Research 11* (2010), 517–553.

[84] Juditsky, A., and Nemirovski, A. On verifiable sufficient conditions for sparse signal recovery via $\ell_1$-minimization. *Mathematical Programming Series B 127*, 1 (2011), 57–88.

[85] Kahale, N. Eigenvalues and expansion of regular graphs. *Journal of the ACM (JACM) 42*, 5 (1995), 1091–1106.

[86] Kashin, B. Diameters of some finite-dimensional sets and classes of smooth functions. *Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya 41*, 2 (1977), 334–351.

[87] Khajehnejad, A., Oymak, S., and Hassibi, B. Subspace expanders and matrix rank minimization. *Arxiv preprint arXiv:1102.3947* (2011).

[88] Kleitman, D. Personal communication. August 2009.

[89] Krahmer, F., and Ward, R. New and improved johnson-lindenstrauss embeddings via the restricted isometry property. *Arxiv preprint arXiv:1009.0744* (2010).

[90] Krishnaiah, P., and Chang, T. On the exact distribution of the smallest root of the wishart matrix using zonal polynomials. *Annals of the Institute of Statistical Mathematics 23*, 1 (1971), 293–295.

[91] Kruskal, J. B. Three-way arrays: Rank and uniqueness of trilinear decompositions, with application to arithmetic complexity and statistics. *Linear Algebra and its Applications 18*, 2 (1977), 95–138.

[92] Ledoux, M. *The concentration of measure phenomenon*, vol. 89. Amer Mathematical Society, 2001.

[93] Li, W. Small value probabilities: techniques and applications. *Lecture notes in Harbin Institute of Technology, to appear* (2010).

[94] Lounici, K., Pontil, M., Tsybakov, A., and Van De Geer, S. Taking advantage of sparsity in multi-task learning. *Arxiv preprint arXiv:0903.1468* (2009).

[95] Lubotzky, A., Phillips, R., and Sarnak, P. Ramanujan graphs. *Combinatorica 8*, 3 (1988), 261–277.

[96] Luby, M., Mitzenmacher, M., Shokrollahi, M., and Spielman, D. Improved low-density parity-check codes using irregular graphs. *IEEE Transactions on Information Theory 47*, 2 (2001), 585–598.

[97] Lustig, M., Donoho, D., Santos, J., and Pauly, J. Compressed sensing MRI. *IEEE Signal Processing Magazine 25*, 2 (2008), 72–82.

[98] Mahoor, M., Zhou, M., Veon, K., Mavadati, S., and Cohn, J. Facial action unit recognition with sparse representation. In *Proceedings of the IEEE International Conference on Automatic Face & Gesture Recognition and Workshops, 2011. FG 2011.* (2011), IEEE, pp. 336–342.

[99] Marčenko, V., and Pastur, L. Distribution of eigenvalues for some sets of random matrices. *Mathematics of the USSR-Sbornik 1* (1967), 457.

[100] Edinburgh Compressed Sensing. http://ecos.maths.ed.ac.uk.

[101] Small Deviations for Stochastic Processes and Related Topics.
http://www.proba.jussieu.fr/pageperso/smalldev/index.html.

[102] Mehta, M. *Random matrices*, vol. 142. Academic press, 2004.

[103] Mendelson, S., Pajor, A., and Tomczak-Jaegermann, N. Reconstruction and subgaussian operators in asymptotic geometric analysis. *Geometric and Functional Analysis 17* (August 2007), 1248–1282.

[104] Mendelson, S., Pajor, A., and Tomczak-Jaegermann, N. Uniform uncertainty principle for bernoulli and subgaussian ensembles. *Constructive Approximation 28*, 3 (2008), 277–289.

[105] Mo, Q., and Li, S. New bounds on the restricted isometry constant $\delta_{2k}$. *Applied and Computational Harmonic Analysis* (2011).

[106] Mo, Q., and Shen, Y. Remarks on the restricted isometry property in orthogonal matching pursuit algorithm. *Arxiv preprint arXiv:1101.4458* (2011).

[107] Muirhead, R. *Aspects of multivariate statistical theory*, vol. 42. Wiley Online Library, 1982.

[108] Natarajan, B. K. Sparse approximate solutions to linear systems. *SIAM Journal on Computing 24*, 2 (1995), 227–234.

[109] Needell, D., and Tropp, J. Cosamp: Iterative signal recovery from incomplete and inaccurate samples. *Applied and Computational Harmonic Analysis 26*, 3 (2009), 301–321.

[110] Parvaresh, F., and Vardy, A. Correcting errors beyond the guruswami-sudan radius in polynomial time. In *Proceedings of 46th Annual IEEE Symposium on Foundations of Computer Science, 2005. FOCS 2005.* (2005), IEEE, pp. 285–294.

[111] Peleg, D., and Upfal, E. Constructing disjoint paths on expander graphs. *Combinatorica 9*, 3 (1989), 289–313.

[112] Pinsker, M. On the complexity of a concentrator. In *Proceedings of the 7th Annual Teletraffic Conference* (1973), p. 318.

[113] Poggio, T., and Shelton, C. On the mathematical foundations of learning. *American Mathematical Society 39*, 1 (2002), 1–49.

[114] Port, S. *Theoretical probability for applications.* Wiley New York, 1994.

[115] Radhakrishnan, J., and Ta-Shma, A. Bounds for dispersers, extractors, and depth-two superconcentrators. *SIAM Journal on Discrete Mathematics 13* (2000), 2.

[116] Rauhut, H. Compressive sensing and structured random matrices. *Theoretical Foundations and Numerical Methods for Sparse Recovery 9* (2010), 1–92.

[117] Raz, R., and Reingold, O. On recycling the randomness of states in space bounded computation. In *Proceedings of the 31st annual ACM symposium on Theory of computing* (1999), ACM, pp. 159–168.

[118] Recht, B., Fazel, M., and Parrilo, P. Guaranteed minimum-rank solutions of linear matrix equations via nuclear norm minimization. *Arxiv preprint arxiv:0706.4138* (2007).

[119] Reingold, O., Vadhan, S., and Wigderson, A. Entropy waves, the zig-zag graph product, and new constant-degree expanders and extractors. In *Proceedings of the 41st Annual Symposium on Foundations of Computer Science, 2000.* (2000), IEEE, pp. 3–13.

[120] Romberg, J. Imaging via compressive sampling. *IEEE Signal Processing Magazine 25*, 2 (2008), 14–20.

[121] Rudelson, M., and Vershynin, R. Geometric approach to error-correcting codes and reconstruction of signals. *International Mathematics Research Notices 2005*, 64 (2005), 4019–4041.

[122] Sapatinas, T. Statistics for high-dimensional data.

[123] Sarvotham, S., and Baraniuk, R. Deterministic bounds for restricted isometry of compressed sensing matrices. *Arxiv preprint arXiv:1103.3316* (2011).

[124] Shannon, C. Communication in the presence of noise. *Proceedings of the Institute of Radio Engineers (IRE) 37*, 1 (1949), 10–21.

[125] Silverstein, J. W. The smallest eigenvalue of a large-dimensional Wishart matrix. *The Annals of Probability 13*, 4 (1985), 1364–1368.

[126] Sipser, M., and Spielman, D. Expander codes. *IEEE Transactions on Information Theory 42*, 6 (1996), 1710–1722.

[127] Smale, S. On the efficiency of algorithms of analysis. *Bulletin of the American Mathematical Society (NS) 13* (1985).

[128] Spielman, D. Linear-time encodable and decodable error-correcting codes. *IEEE Transactions on Information Theory 42*, 6 (1996), 1723–1731.

[129] Stankovic, V., Stankovic, L., and Cheng, S. Compressive video sampling. In *Proceedings of the European Signal Processing Conference (EUSIPCO)* (2008), Citeseer.

[130] Sugiyama, T. On the distribution of the largest latent root of the covariance matrix. *The Annals of Mathematical Statistics* (1967), 1148–1151.

[131] Szarek, S. J. Condition numbers of random matrices. *Journal of Complexity 7* (1991), 131–149.

[132] Ta-Shma, A., Umans, C., and Zuckerman, D. Loss-less condensers, unbalanced expanders, and extractors. In *Proceedings of the 33rd annual ACM symposium on Theory of computing* (2001), ACM, pp. 143–152.

[133] Takhar, D., Bansal, V., Wakin, M., Duarte, M., Baron, D., Kelly, K., and Baraniuk, R. A compressed sensing camera: New theory and an implementation using digital micromirrors. *Proceedings of Computational Imaging IV at SPIE Electronic Imaging, San Jose* (2006).

[134] Talagrand, M. *The generic chaining.* Springer, 2005.

[135] Tanner, R. Explicit concentrators from generalized $n$-gons. *SIAM Journal on Algebraic and Discrete Methods 5* (1984), 287.

[136] Tao, T., and Vu, V. Random matrices: Universality of local eigenvalue statistics. *Acta Mathematica* (2011), 1–78.

[137] Tao, T., Vu, V., and Krishnapur, M. Random matrices: Universality of ESDs and the circular law. *The Annals of Probability 38*, 5 (2010), 2023–2065.

[138] Temlyakov, V. Nonlinear methods of approximation. *Foundations of Computational Mathematics 3*, 1 (2003), 33–107.

[139] Tibshirani, R. Regression shrinkage and selection via the lasso. *Journal of the Royal Statistical Society. Series B (Methodological)* (1996), 267–288.

[140] Traub, J. Information-based complexity.

[141] Trefethen, L., and Bau, D. *Numerical linear algebra.* No. 50. Society for Industrial Mathematics, 1997.

[142] Trefethen, L., and Schreiber, R. Average-case stability of gaussian elimination. *SIAM Journal on Matrix Analysis and Applications 11* (1990), 335.

[143] Tropp, J., and Gilbert, A. Signal recovery from random measurements via orthogonal matching pursuit. *IEEE Transactions on Information Theory 53*, 12 (2007), 4655–4666.

[144] Von Neumann, J., and Goldstine, H. Numerical inverting of matrices of high order. *Bulletin of the American Mathematical Society 53*, 11 (1947), 1021–1099.

[145] Whittaker, E., and Watson, G. *A course of modern analysis: an introduction to the general theory of infinite processes and of analytic functions, with an account of the principal transcendental functions.* Cambridge University Press, 1927.

[146] Wigner, E. On the distribution of the roots of certain symmetric matrices. *The Annals of Mathematics 67*, 2 (1958), 325–327.

[147] Wright, J., Ma, Y., Mairal, J., Sapiro, G., Huang, T., and Yan, S. Sparse representation for computer vision and pattern recognition. *Proceedings of the IEEE 98*, 6 (2010), 1031–1044.

[148] Xu, W., and Hassibi, B. Efficient compressive sensing with deterministic guarantees using expander graphs. In *Proceedings of the IEEE Information Theory Workshop, 2007. ITW'07.* (2007), IEEE, pp. 414–419.

[149] Xu, W., and Hassibi, B. Further results on performance analysis for compressive sensing using expander graphs. In *Conference Record of the 41st Asilomar Conference on Signals, Systems and Computers, 2007. ACSSC 2007.* (2007), IEEE, pp. 621–625.

[150] Zou, H., Hastie, T., and Tibshirani, R. Sparse principal component analysis. *Journal of Computational and Graphical Statistics 15*, 2 (2006), 265–286.