

Vanishingly Sparse Matrices and Expander Graphs, with application to compressed sensing

Bubacarr Bah, and Jared Tanner,

Abstract—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 neighbors* for these graphs, and present tail bounds on the probability that this cardinality will be less than the expected value. Deducible from these bounds are similar bounds 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. The exponential tail bounds yield the best known bounds for the ℓ_1 norm of large rectangular matrices when restricted to act on vectors with few nonzeros; this quantity is referred to as the ℓ_1 norm restricted isometry constants (RIC_1) of the matrix. These bounds allow for quantitative theorems on existence of expander graphs and hence the sparse random matrices we consider and also quantitative compressed sensing sampling theorems when using sparse non-mean-zero measurement matrices.

Index Terms—Algorithms, compressed sensing, signal processing, sparse matrices, expander graphs.

I. INTRODUCTION

Sparse matrices are particularly useful in applied and computational mathematics because of their low storage complexity and fast implementation as compared to dense matrices, see [1], [2], [3]. Of late, significant progress has been made to incorporate sparse matrices in compressed sensing, with [4], [5], [6], [7] giving both theoretical performance guarantees and also exhibiting numerical results that shows sparse matrices coming from expander graphs can be as good sensing matrices as their dense counterparts. In fact, Blanchard and Tanner [8] 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 (as considered here).

In this manuscript we consider random sparse matrices that are adjacency matrices of lossless expander graphs. Expander graphs are highly connected graphs with very sparse adjacency matrices, a precise definition of a lossless expander graph is given in Definition 1.1 and their diagrammatic illustration in Figure 1.

Definition 1.1: $G = (U, V, E)$ is a lossless (k, d, ϵ) -expander if it is a bipartite graph with $|U| = N$ left vertices, $|V| = n$ right vertices and has a regular left degree d , such

that any $X \subset U$ with $|X| \leq k$ has $|\Gamma(X)| = (1 - \epsilon)d|X|$ neighbors.¹

- Remark 1.2:** 1) The graphs are *lossless* because $\epsilon \ll 1$;
2) They are called *unbalanced expanders* when $n \ll N$;
3) The *expansion* of a lossless (k, d, ϵ) -expander graph is $(1 - \epsilon)d$.

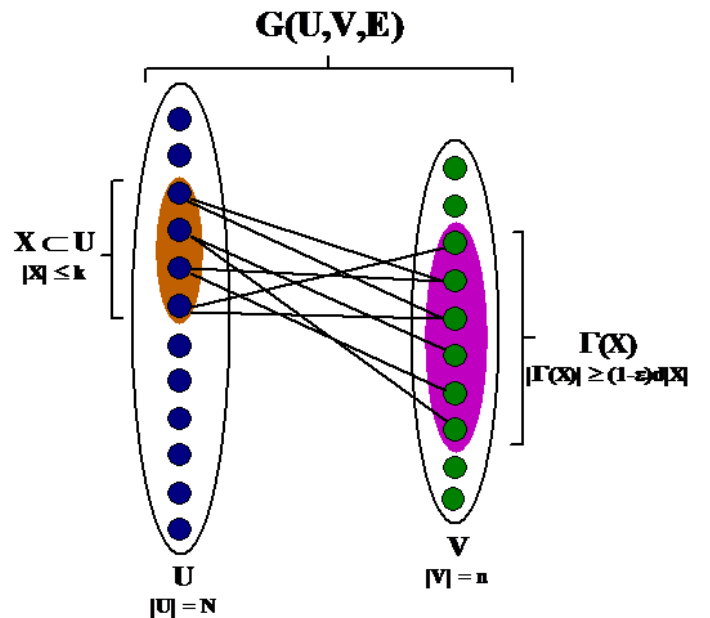


Fig. 1. Illustration of a lossless (k, d, ϵ) -expander graphs with $k = 4$ and $d = 2$.

Such graphs have been well studied in theoretical computer science and pure mathematics and have many applications including: Distributed Routing in Networks, Linear Time Decodable Error-Correcting Codes, Bitprobe Complexity of Storing Subsets, Fault-tolerance and a Distributed Storage Method, and Hard Tautologies in Proof Complexity, see [10] or [9] for a more detailed survey. Pinsker and Bassylago [11] proved the existence of lossless expanders and showed that any random left-regular bipartite graph is, with high probability, an expander graph. Probabilistic constructions with optimal parameters n, N exist but are not suitable for the applications we consider here. Deterministic constructions only achieve sub-optimal parameters, see Guruswami et. al. [12].

Our main contribution, is the presentation of quantitative guarantees on the probabilistic construction of these objects in the form of a bound on the tail probability of the size of

School of Mathematics and Maxwell Institute, University of Edinburgh, Edinburgh, UK (b.bah@sms.ed.ac.uk).

Mathematics Institute and Exeter College, University of Oxford, Oxford, UK (tanner@maths.ox.ac.uk). JT acknowledges support from the Leverhulme Trust.

¹Lossless 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 [9], [5] and the references therein.

the *set of neighbors*, $\Gamma(X)$ for a given $X \subset U$, of a randomly generated left-degree bipartite graph. Moreover, we provide deducible bounds on the tail probability of the *expansion* of the graph, $|\Gamma(X)|/|X|$. We derive quantitative guarantees for randomly generated non-mean zero sparse binary matrices to be adjacency matrices of expander graphs. In addition, we derive the first phase transitions showing regions in parameter space that depicting when a left-regular bipartite graph with a given set of parameters is guaranteed to be a lossless expander with high probability. The key innovation in this paper is the use of a novel technique of *dyadic splitting of sets*. We derived our bounds using this technique and apply them to derive ℓ_1 restricted isometry constants (RIC_1).

Numerous compressed sensing algorithms have been designed for sparse matrices [4], [5], [6], [7]. Another contribution of our work is the derivation of sampling theorems, presented as phase transitions, comparing performance guarantees for some of these algorithms as well as the more traditional ℓ_1 minimization compressed sensing formulation. We also show how favorably ℓ_1 minimization performance guarantees for such sparse matrices compared to what ℓ_2 restricted isometry constants (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. [13] that provided such theorems for dense Gaussian matrices based on RIC_2 analysis.

The outline of the rest of this introduction section goes as follows. In Section I-A we present our main results in Theorem 1.6 and Corollary 1.7. In Section I-B we discuss RIC_1 and its implication for compressed sensing, leading to two sampling theorems in Corollaries 1.10 and 1.11.

A. Main results

Our main results is 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 a key concept of a *set of neighbors* used in the derivation of the main results of the manuscript.

Definition 1.3: 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, ϵ) -expander graphs while SSE matrices have random sign patterns in the nonzeros of an adjacency matrix of a lossless (k, d, ϵ) -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.” We denote A_S as a submatrix of A composed of columns of A indexed by the set S with $|S| = s$. To aid translation between the terminology of graph theory and linear algebra we define the *set of neighbors* in both notation.

Definition 1.4: 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 $S \subset U$ its set of neighbors 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 neighbors of A_S for $|S| = s$, denoted by A_s , is the set of rows with at least one nonzero.

Definition 1.5: Using Definition 1.4 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 1.1, we need $|\Gamma(S)|$ to be large for every small $S \subset U$. In terms of the class of matrices defined by Definition 1.3, 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 1.6 to answers. 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 of some selected compressed sensing algorithms.

Theorem 1.6: 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 1.3, then

$$\text{Prob}(|A_s| \leq a_s) < p_{max}(s, d) \times \exp[n \cdot \Psi(a_s, \dots, a_2, d)] \quad (1)$$

where $p_{max}(s, d)$ is given by

$$p_{max}(s, d) = \frac{2}{25\sqrt{2\pi s^3 d^3}}, \quad \text{and} \quad (2)$$

$$\Psi(a_s, \dots, a_2, d) = \frac{1}{n} \left[\sum_{i=1}^{\lceil s/2 \rceil} \frac{s}{2i} \left((n - a_i) \cdot \text{H}\left(\frac{a_{2i} - a_i}{n - a_i}\right) + a_i \cdot \text{H}\left(\frac{a_{2i} - a_i}{a_i}\right) - n \cdot \text{H}\left(\frac{a_i}{n}\right) \right) + 3s \log(5d) \right] \quad (3)$$

where $a_1 := d$. 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

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

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

$$a_{2i}^3 - 2a_i a_{2i}^2 + 2a_i^2 a_{2i} - a_i^2 a_{4i} = 0 \quad \text{for } i = 1, 2, \dots, \lceil s/4 \rceil \quad (5)$$

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

Corollary 1.7: 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 1.3, then

$$\text{Prob}(\|A_S x\|_1 \leq (1 - 2\epsilon)d\|x\|_1) < p_{max}(s, d) \times \exp[n \cdot \Psi(s, d, \epsilon)] \quad (6)$$

where $\Psi(s, d, \epsilon) = \Psi(a_s, \dots, a_2, d)$ in (3) with $a_s = (1 - \epsilon)ds$ and $p_{max}(s, d)$ is the polynomial in (2).

Theorem 1.6 and Corollary 1.7 allow us to calculate s, n, N, d, ϵ where the probability of the probabilistic constructions in Definition 1.3 not being a lossless (s, d, ϵ) -expander is exponentially small. For moderate values of ϵ this allows us to make quantitative sampling theorems for some compressed sensing reconstruction algorithms.

B. RIC₁ and its implications to Compressed Sensing

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 endeavor to recovery this vector of interest by exploiting the inherent simplicity in this vector. Precisely, let $x \in \mathbb{R}^N$, be the vector of interest whose simplicity is that it has $k < N$ nonzeros, which we refer to as k -sparse; then we observe $y \in \mathbb{R}^n$, as the measurement vector resulting from the multiplication of x by an $n \times N$ matrix, A . The minimum simplicity reconstruct of x can be written as

$$\min_{x \in \chi^N} \|x\|_0 \quad \text{subject to} \quad Ax = y, \quad (7)$$

where χ^N is the set of all k -sparse vectors and $\|z\|_0$ counts the nonzero components of z ; this model may be reformulated to include noise in the measurements. References [14], [15], [16], [17] give detailed introductions to compressed sensing and its applications; while [18], [19], [20], [21], [22], [5], [6], [23], [4], [24] provide information on some of the popular computationally efficient algorithms used to solve problem (7) and its reformulations.

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. $\|x - \hat{x}\|_1 \leq \text{Const.} \|x - x_k\|_1$ where x_k is the optimal k -term representation for x . This is possible if A has small RIC₁, in other words A satisfies the ℓ_1 restricted isometry property (RIP-1), introduced by Berinde et. al. in [5] and defined as thus.

Definition 1.8 (RIP-1): Let χ^N be the set of all k -sparse vectors, then an $n \times N$ matrix A has RIP-1, with the lower RIC₁ being the smallest $L(k, n, N; A)$, when the following condition holds.

$$(1 - L(k, n, N; A)) \|x\|_1 \leq \|Ax\|_1 \leq \|x\|_1 \quad \forall x \in \chi^N. \quad (8)$$

For computational purposes it is preferable to have A sparse, but little quantitative information on $L(k, n, N; A)$ has been available for large sparse rectangular matrices. Berinde et. al. in [5] showed that scaled adjacency matrices of lossless expander graphs (i.e. scaled SE matrices) satisfy RIP-1, and the same proof extends to the signed adjacency matrices (i.e. so called SSE matrices).

Theorem 1.9: If an $n \times N$ matrix A is either SE or SSE defined in Definition 1.3, then A/d satisfies RIP-1 with $L(k, n, N; A) = 2\epsilon$.

Proof: The proof of the signed case (SSE) follows that of the unsigned case (SE) in [5] but with absolute values included in the appropriate stages. ■

Based on Theorem 1.9 which guarantees RIP-1, (8), for the class of matrices in Definition 1.3, we give a bound, in Corollary 1.10, for the probability that a random draw of a matrix with d 1s or ± 1 s 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 1.3. In addition to Theorem 1.9, Corollary 1.10 follows from Theorem 1.6 and Corollary 1.7.

Corollary 1.10: Considering RIP-1, if A is drawn from the class of matrices in Definition 1.3 and any k -sparse vector x with k, n, N and $0 < \epsilon < 1/2$ fixed, then

$$\text{Prob}(\|Ax\|_1 \leq (1 - 2\epsilon)d\|x\|_1) < p'_{max}(N, k, d) \times \exp[N \cdot \Psi_{net}(k, n, N; d, \epsilon)] \quad (9)$$

where $p'_{max}(N, k, d)$ and Ψ_{net} are given by

$$p'_{max}(N, k, d) = \frac{1}{16\pi k \sqrt{d^3 \left(1 - \frac{k}{N}\right)}}, \quad (10)$$

$$\Psi_{net}(k, n, N; d, \epsilon) = \text{H}\left(\frac{k}{N}\right) + \frac{n}{N} \Psi(k, d, \epsilon), \quad (11)$$

with $\Psi(k, d, \epsilon)$ defined in Corollary 1.7.

Furthermore, the following corollary is a consequence of Corollary 1.10 and it is a sampling theorem on the existence of lossless expander graphs. The proof of Corollaries 1.10 and 1.11 are presented in Sections IV-B2 and IV-B3 respectively.

Corollary 1.11: Consider $0 < \epsilon < 1/2$ and d fixed. If A is drawn from the class of matrices in Definition 1.3 and any x drawn from χ^N with $(k, n, N) \rightarrow \infty$ while $k/n \rightarrow \rho \in (0, 1)$ and $n/N \rightarrow \delta \in (0, 1)$ then for $\rho < (1 - \gamma)\rho^{exp}(\delta; d, \epsilon)$ and $\gamma > 0$

$$\text{Prob}(\|Ax\|_1 \geq (1 - 2\epsilon)d\|x\|_1) \rightarrow 1 \quad (12)$$

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

$$\text{H}\left(\frac{k}{N}\right) + \frac{n}{N} \Psi(k, d, \epsilon) = 0. \quad (13)$$

The outline of the rest of the manuscript is as follows: In Section II 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 1.6. In Section III we discuss restricted isometry constants and compressed sensing algorithms. In Section IV we prove the main results, that is Theorem 1.6 and the corollaries in Sections I-A and I-B. Section V is the appendix where we present the alternative to Theorem 1.6.

II. 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 II-A, numerical results that support the claims of the main results in Sections I-A and I-B. This is followed in Section II with lemmas, propositions and corollaries and their proofs.

A. Discussion on main results

Theorem 1.6 gives a bound on the probability that the cardinality of a union of k sets each with d elements is less than a_k . Figure 2 shows plots of values of a_k (size of set of neighbors) 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, Figure 3 also shows values of a_k/k (the graph expansion) also taken over 500 realizations.

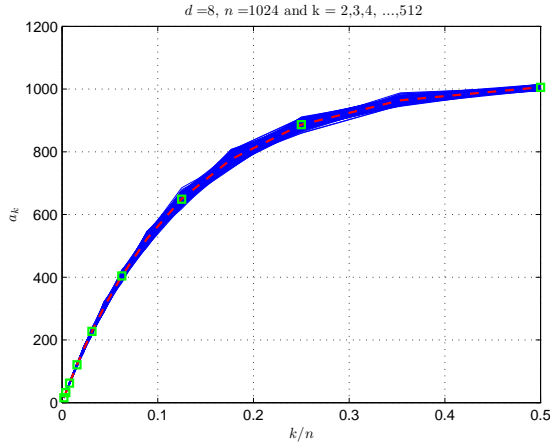


Fig. 2. For fixed $d = 8$ and $n = 2^{10}$, over 500 realizations we plot (in blue) the cardinalities of the index sets of nonzeros in a given number of set sizes, k . The dotted red curve is mean of the simulations and the green squares are the \hat{a}_k .

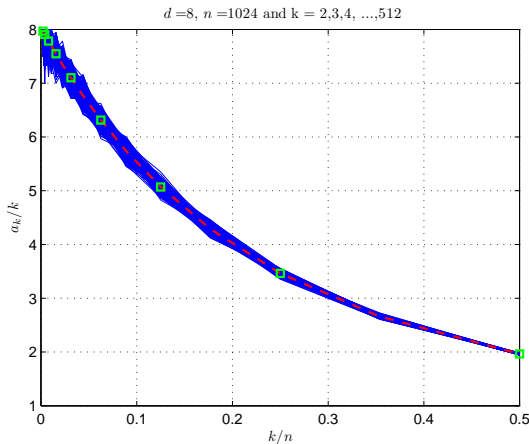


Fig. 3. For fixed $d = 8$ and $n = 2^{10}$, over 500 realizations we plot (in blue) the graph expansion for a given input set size k . The dotted red curve is mean of the simulations and the green squares are the \hat{a}_k/k .

Theorem 1.6 also claims that the \hat{a}_s are the expected values of the cardinalities of the union of s sets. We given a brief proof sketch of its proof in Section II-B in terms of the maximum likelihood and empirical illustrate the accuracy of the result in Figure 4 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} .

Figure 5 shows representative values of a_i from (5) for $a_k := (1 - \epsilon)\hat{a}_k$ as a function of ϵ for $d = 8$, $k = 2 \times 10^3$, and $n = 2^{20}$. Each of the a_i decrease smoothly towards d ,

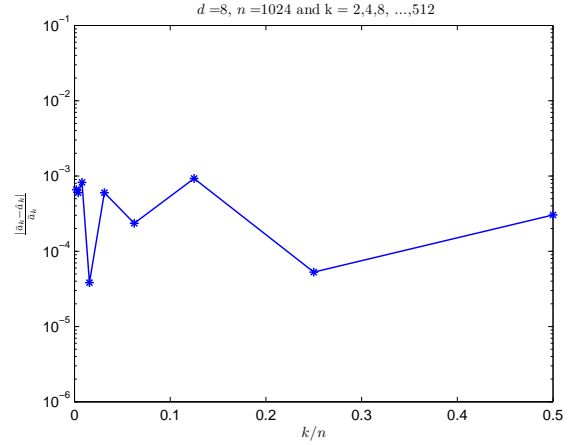


Fig. 4. For fixed $d = 8$ and $n = 2^{10}$, over 500 realizations the relative error between the mean values of a_k (referred to as \bar{a}_k) and the \hat{a}_k from Equation (4) of Theorem 1.6.

but with a_i for smaller values if i varying less than for larger values of i .

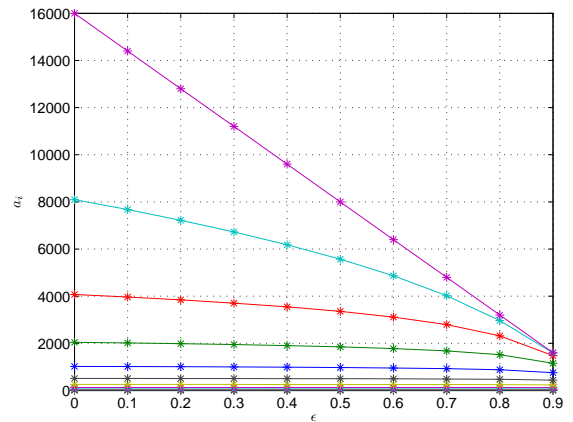


Fig. 5. Values of a_i as a function of $\epsilon \in [0, 1)$ for $a_k := (1 - \epsilon)\hat{a}_k$ with $d = 8$, $k = 2 \times 10^3$ and $n = 2^{20}$. For this choice of d, k, n there are twelve levels of dyadic splits resulting in a_i for $i = 2^j$ for $j = 0, \dots, \lceil \log_2 k \rceil = 12$. The 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.

For fixed $0 < \epsilon < 1/2$ and for small but fixed d , $\rho^{exp}(\delta; d, \epsilon)$ in Corollary 1.11 is a function of δ for each d and ϵ , is a phase transition function in the (δ, ρ) plane. Below the curve of $\rho^{exp}(\delta; d, \epsilon)$ the probability in (12) goes to one exponentially in n as the problem size grows. That is if A is drawn at random with d 1s or $d \pm 1$ s 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 1.3 with probability approaching one exponentially in n . In terms of $|\Gamma(X)|$ for $X \subset U$ and $|X| \leq k$, Corollary 1.11 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, ϵ) -expander. Figure 6 shows a plot of what $\rho^{exp}(\delta; d, \epsilon)$

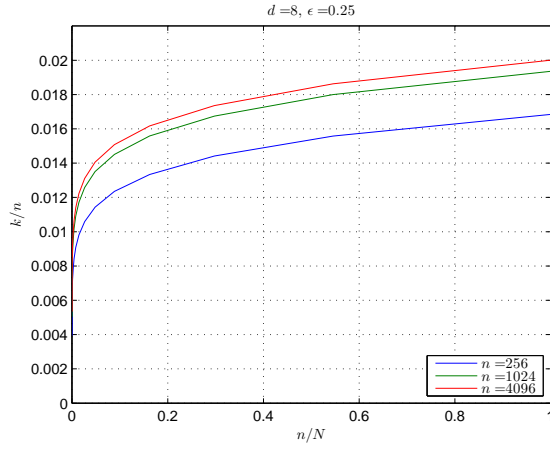


Fig. 6. Phase transition plots of $\rho^{exp}(\delta; d, \epsilon)$ for fixed $d = 8$ and $\epsilon = 1/4$ with n varied.

converge to for different values of n with ϵ and d fixed; Figure 7 shows a plot of what $\rho^{exp}(\delta; d, \epsilon)$ converge to for different values of d with ϵ and n fixed; while Figure 8 shows plots of what $\rho^{exp}(\delta; d, \epsilon)$ converge to for different values of ϵ with n and d 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 [8] 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.

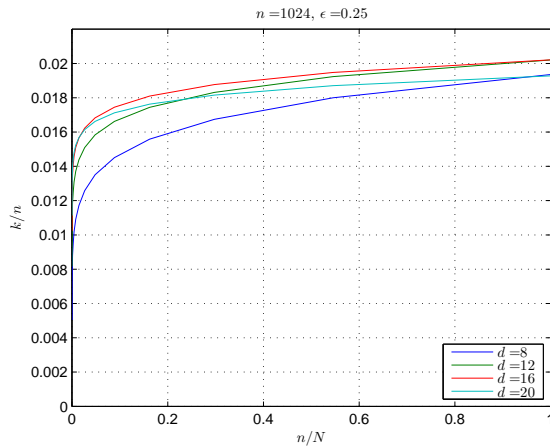


Fig. 7. Phase transition plots of $\rho^{exp}(\delta; d, \epsilon)$ for fixed $\epsilon = 1/6$ and $n = 2^{10}$ with d varied.

As afore-stated Corollary 1.11 follows from Theorem 1.6, alternatively Corollary 1.11 can be arrived at based on probabilistic constructions of expander graphs given by Proposition

2.1 below. This proposition and its proof can be traced back to Pinsker in [25] but more recent proofs can be found in [6], [10].

Proposition 2.1: For any $N/2 \geq k \geq 1$, $\epsilon > 0$ there exists a lossless (k, d, ϵ) -expander with

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

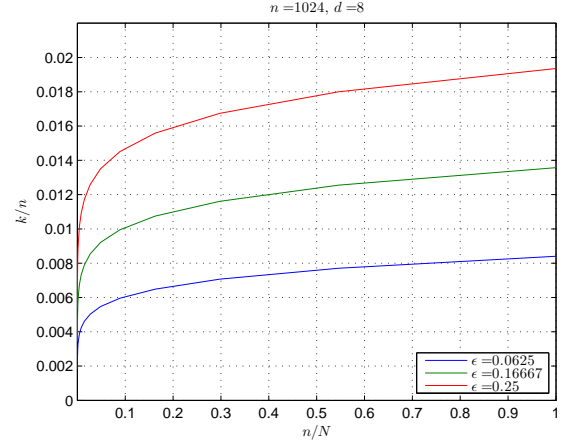


Fig. 8. Phase transition plots of $\rho^{exp}(\delta; d, \epsilon)$ for fixed $d = 8$ and $n = 2^{10}$ with ϵ varied.

To put our results in perspective, we compare them to the alternative construction in [6] which led to Corollary 2.2, whose proof is given in Section V-A of the Appendix. Figure 9 compares the phase transitions resulting from our construction to that presented in [6], but we must point out however, that the proof in [6] was not aimed for a tight bound.

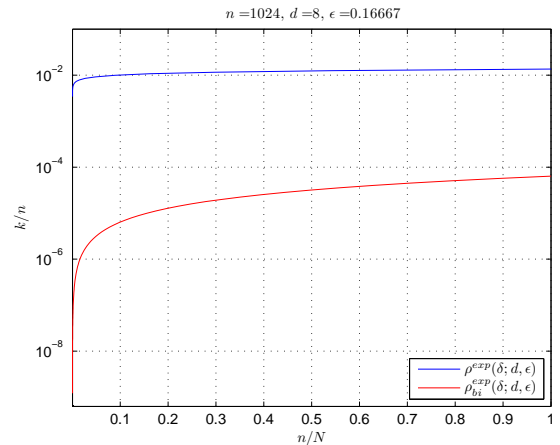


Fig. 9. A comparison of ρ^{exp} in Theorem 1.6 to ρ_{bi}^{exp} of Corollary 2.2 derived using the construction based on Corollary 2.2.

Corollary 2.2: 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 $(k, n, N) \rightarrow \infty$ while $k/n \rightarrow \rho \in (0, 1)$ and $n/N \rightarrow \delta \in (0, 1)$ then for $\rho < (1 - \gamma)\rho_{bi}^{exp}(\delta; d, \epsilon)$ and $\gamma > 0$

$$\text{Prob}(G \text{ fails to be an expander}) \rightarrow 0 \quad (14)$$

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

$$\Psi(k, n, N; d, \epsilon) = 0 \quad (15)$$

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

B. 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 IV.

For one fixed set of columns of A , denoted A_S , the probability in (1) can be understood as the cardinality of the unions 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 it's 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 (1) involves the computation of the probability of the cardinality of the intersection of two sets. This probability is given by Lemma 2.3 and Corollary 2.4 below.

Lemma 2.3: 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 $P_n(b, b_1, b_2) := \text{Prob}(|B_1 \cap B_2| = b_1 + b_2 - b)$, then

$$P_n(b, b_1, b_2) = \binom{b_1}{b_1 + b_2 - b} \binom{n - b_1}{b - b_1} \binom{n}{b_2}^{-1}. \quad (16)$$

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 (16). ■

Corollary 2.4: If two sets, $B_1, B_2 \subset [n]$ are drawn uniformly at random, independent of each other, and $B = B_1 \cup B_2$

$$\begin{aligned} \text{Prob}(|B| = b) &= P_n(b, b_1, b_2) \times \\ &\text{Prob}(|B_1| = b_1) \cdot \text{Prob}(|B_2| = b_2) \end{aligned} \quad (17)$$

Proof: $\text{Prob}(|B| = b) = \text{Prob}(|B_1 \cup B_2| = b)$ by definition. As a consequence of the inclusion-exclusion principle

$$\begin{aligned} \text{Prob}(|B_1 \cup B_2| = b) &= \text{Prob}(|B_1 \cap B_2| = b_1 + b_2 - b) \\ &\times \text{Prob}(|B_1| = b_1) \cdot \text{Prob}(|B_2| = b_2). \end{aligned} \quad (18)$$

We use Lemma 2.3 to replace $\text{Prob}(|B_1 \cap B_2| = b_1 + b_2 - b)$ in (18) by $P_n(b, b_1, b_2)$ 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 (1). We state and prove what we refer to a *dyadic splitting lemma*, Lemma 2.5, 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 2.5: Let S be an index set of cardinality s . For any level j of the dyadic splitting, $j = 0, \dots, \lceil \log_2 s \rceil - 1$, the set S is decomposed into disjoint sets each having cardinality $Q_j = \lceil \frac{s}{2^j} \rceil$ or $R_j = Q_j - 1$. Let q_j sets have cardinality Q_j and r_j sets have cardinality R_j , then

$$q_j = s - 2^j \cdot \left\lceil \frac{s}{2^j} \right\rceil + 2^j, \quad \text{and} \quad r_j = 2^j - q_j. \quad (19)$$

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.

$$Q_j = \frac{s}{2^j} + \frac{m_1}{2^j} \quad \text{and} \quad R_j = \frac{s}{2^j} + \frac{m_2}{2^j}. \quad (20)$$

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

$$\frac{m_1 - m_2}{2^j} = 1. \quad (21)$$

Now let q_j and r_j be the number of children with Q_j and R_j number of columns respectively. Therefore,

$$q_j + r_j = 2^j. \quad (22)$$

At each level j of the splitting the following condition must be satisfied

$$q_j \cdot Q_j + r_j \cdot R_j = s. \quad (23)$$

To find m_1, m_2, q_j and r_j , from (20) we substitute for Q_j and R_j in (23) to have

$$q_j \cdot \left(\frac{s}{2^j} + \frac{m_1}{2^j}\right) + r_j \cdot \left(\frac{s}{2^j} + \frac{m_2}{2^j}\right) = s, \quad (24)$$

$$2^{-j} q_j s + 2^{-j} q_j m_1 + 2^{-j} r_j s + 2^{-j} r_j m_2 = s, \quad (25)$$

$$2^{-j} (q_j + r_j) s + 2^{-j} (q_j m_1 + r_j m_2) = s, \quad (26)$$

$$s + 2^{-j} (q_j m_1 + r_j m_2) = s, \quad (27)$$

$$q_j m_1 + r_j m_2 = 0. \quad (28)$$

We expanded the brackets from (24) to (25) and simplified from (25) to (26). We simplify the first term of (26) using (22) to get (27) and we simplified this to get (28).

Equation (21) yields

$$m_1 = m_2 + 2^j. \quad (29)$$

Substituting this in (28) yields

$$q_j (m_2 + 2^j) + r_j m_2 = 0, \quad (30)$$

$$(q_j + r_j) m_2 + 2^j q_j = 0, \quad (31)$$

$$2^j (q_j + m_2) = 0. \quad (32)$$

From (30) to (31) we expanded the brackets and rearranged the terms and used (22) to simplify to (32). Using (32) and (29) respectively we have

$$m_2 = -q_j \quad \text{and} \quad m_1 = 2^j - q_j = r_j. \quad (33)$$

Substituting this in (20) we have

$$Q_j = \frac{s - q_j}{2^j} + 1 \quad \text{and} \quad R_j = \frac{s - q_j}{2^j}. \quad (34)$$

Equating this value of Q_j to its defined value in the statement of the lemma gives

$$\frac{s - q_j}{2^j} + 1 = \left\lceil \frac{s}{2^j} \right\rceil \Rightarrow q_j = s - 2^j \cdot \left\lceil \frac{s}{2^j} \right\rceil + 2^j. \quad (35)$$

Therefore, from (33) we use (35) to have

$$r_j = 2^j - q_j \Rightarrow r_j = 2^j \cdot \left\lceil \frac{s}{2^j} \right\rceil - s, \quad (36)$$

which concludes the proof. \blacksquare

The bound in (1) is derived using a large deviation analysis of the nested probabilities which follow from the dyadic splitting in Corollary 2.4. The large deviation analysis of (16) at each stage involves its large deviation exponent $\psi_n(\cdot)$, which follows from Stirling's inequality bounds on the combinatorial product of (16). Lemma 2.6 establishes a few properties of $\psi_n(\cdot)$ while Lemma 2.7 shows how the various $\psi_n(\cdot)$'s at a given dyadic splitting level can be combined into a relatively simple expression.

Lemma 2.6: Define

$$\psi_n(x, y, z) := y \cdot \mathbf{H}\left(\frac{x-z}{y}\right) + (n-y) \cdot \mathbf{H}\left(\frac{x-y}{n-y}\right) - n \cdot \mathbf{H}\left(\frac{z}{n}\right), \quad (37)$$

then for $n > x > y$ we have that

$$\text{for } y > z \quad \psi_n(x, y, y) \leq \psi_n(x, y, z) \leq \psi_n(x, z, z); \quad (38)$$

$$\text{for } x > z \quad \psi_n(x, y, y) > \psi_n(z, y, y); \quad (39)$$

$$\text{for } 1/2 < \alpha \leq 1 \quad \psi_n(x, y, y) < \psi_n(\alpha x, \alpha y, \alpha y). \quad (40)$$

Proof: We start with Property (38) and first show that the left inequality holds. If we substitute y for z in (37) with $y > z$ we reduce the first and last terms of (37) while we increase the middle term of (37) which makes $\psi_n(x, y, y) \leq \psi_n(x, y, z)$. For second inequality we replace y by z in (37) with $y > z$ we increase the first and the last terms of (37) and reduce the middle term which makes $\psi_n(x, y, z) \leq \psi_n(x, z, z)$. This concludes the proof for (38).

Property (39) states that for fixed y , $\psi_n(x, y, y)$ is monotonically increasing in its first argument. To prove (39) we use the condition $n > x > y$ to ensure that $\mathbf{H}(p)$ increases monotonically with p , which implies that the first and last terms of (37) increase with x for fixed y while the second term remains constant.

Property (40) 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 (37) we write out clearly what the difference, $\psi_n(\alpha x, \alpha y, \alpha y) - \psi_n(x, y, y)$, is as follows.

$$\begin{aligned} & \alpha y \mathbf{H}\left(\frac{\alpha x - \alpha y}{\alpha y}\right) + (n - \alpha y) \mathbf{H}\left(\frac{\alpha x - \alpha y}{n - \alpha y}\right) - n \mathbf{H}\left(\frac{\alpha y}{n}\right) \\ & - y \mathbf{H}\left(\frac{x - y}{y}\right) - (n - y) \mathbf{H}\left(\frac{x - y}{n - y}\right) + n \mathbf{H}\left(\frac{y}{n}\right) \end{aligned} \quad (41)$$

$$\begin{aligned} & = \alpha y \mathbf{H}\left(\frac{x - y}{y}\right) + n \mathbf{H}\left(\frac{\alpha x - \alpha y}{n - \alpha y}\right) - \alpha y \mathbf{H}\left(\frac{\alpha x - \alpha y}{n - \alpha y}\right) \\ & - n \mathbf{H}\left(\frac{\alpha y}{n}\right) - y \mathbf{H}\left(\frac{x - y}{y}\right) - n \mathbf{H}\left(\frac{x - y}{n - y}\right) \\ & + y \mathbf{H}\left(\frac{x - y}{n - y}\right) + n \mathbf{H}\left(\frac{y}{n}\right) \end{aligned} \quad (42)$$

$$\begin{aligned} & = \alpha y \mathbf{H}\left(\frac{x - y}{y}\right) - \alpha y \mathbf{H}\left(\frac{\alpha x - \alpha y}{n - \alpha y}\right) - y \mathbf{H}\left(\frac{x - y}{y}\right) \\ & + y \mathbf{H}\left(\frac{x - y}{n - y}\right) + n \mathbf{H}\left(\frac{y}{n}\right) - n \mathbf{H}\left(\frac{\alpha y}{n}\right) \\ & + n \mathbf{H}\left(\frac{\alpha x - \alpha y}{n - \alpha y}\right) - n \mathbf{H}\left(\frac{x - y}{n - y}\right) \end{aligned} \quad (43)$$

From (41) to (42) we expanded brackets and simplified, while from (42) to (43) we rearranged the terms for easy comparison.

Again $n > x > y$ ensures that the arguments of $\mathbf{H}(\cdot)$ are strictly less than half and $\mathbf{H}(p)$ increases monotonically with p . In (43) 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 α 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 2.6. \blacksquare

Lemma 2.7: Given $\psi_n(\cdot)$ as defined in (37) then the following bound holds.

$$\begin{aligned} & \sum_{j=0}^{\lceil \log_2(s) \rceil - 2} \left[q_j \cdot \psi_n \left(a_{Q_j}, a_{\lceil \frac{Q_j}{2} \rceil}, a_{\lfloor \frac{Q_j}{2} \rfloor} \right) + \right. \\ & \left. r_j \cdot \psi_n \left(a_{R_j}, a_{\lceil \frac{R_j}{2} \rceil}, a_{\lfloor \frac{R_j}{2} \rfloor} \right) \right] + q_{\lceil \log_2(s) \rceil - 1} \cdot \psi_n(a_2, d, d) \\ & \leq \sum_{j=0}^{\lceil \log_2(s) \rceil - 1} 2^j \cdot \psi_n \left(a_{Q_j}, a_{\lfloor \frac{R_j}{2} \rfloor}, a_{\lfloor \frac{R_j}{2} \rfloor} \right), \end{aligned} \quad (44)$$

where $a_{\lfloor \frac{R_{\lceil \log_2(s) \rceil - 1}}{2} \rfloor} = d$.

Proof: The quantity inside the left hand side summation

in (44), i.e.

$$q_j \cdot \psi_n \left(a_{Q_j}, a_{\lceil \frac{Q_j}{2} \rceil}, a_{\lfloor \frac{Q_j}{2} \rfloor} \right) + r_j \cdot \psi_n \left(a_{R_j}, a_{\lceil \frac{R_j}{2} \rceil}, a_{\lfloor \frac{R_j}{2} \rfloor} \right), \quad (45)$$

is equal to the following if we replace q_j and r_j by their values given in Lemma 2.5.

$$\left(s - 2^j \left\lceil \frac{s}{2^j} \right\rceil + 2^j \right) \cdot \psi_n \left(a_{Q_j}, a_{\lceil \frac{Q_j}{2} \rceil}, a_{\lfloor \frac{Q_j}{2} \rfloor} \right) \quad (46)$$

$$+ \left(2^j \left\lceil \frac{s}{2^j} \right\rceil - s \right) \cdot \psi_n \left(a_{R_j}, a_{\lceil \frac{R_j}{2} \rceil}, a_{\lfloor \frac{R_j}{2} \rfloor} \right) < \left(s - 2^j \left\lceil \frac{s}{2^j} \right\rceil + 2^j \right) \cdot \psi_n \left(a_{Q_j}, a_{\lceil \frac{Q_j}{2} \rceil}, a_{\lfloor \frac{Q_j}{2} \rfloor} \right) \quad (47)$$

$$+ \left(2^j \left\lceil \frac{s}{2^j} \right\rceil - s \right) \cdot \psi_n \left(a_{R_j}, a_{\lceil \frac{R_j}{2} \rceil}, a_{\lfloor \frac{R_j}{2} \rfloor} \right) < \left(s - 2^j \left\lceil \frac{s}{2^j} \right\rceil + 2^j \right) \cdot \psi_n \left(a_{Q_j}, a_{\lceil \frac{R_j}{2} \rceil}, a_{\lfloor \frac{R_j}{2} \rfloor} \right) \quad (48)$$

$$+ \left(2^j \left\lceil \frac{s}{2^j} \right\rceil - s \right) \cdot \psi_n \left(a_{R_j}, a_{\lceil \frac{R_j}{2} \rceil}, a_{\lfloor \frac{R_j}{2} \rfloor} \right) < \left(s - 2^j \left\lceil \frac{s}{2^j} \right\rceil + 2^j \right) \cdot \psi_n \left(a_{Q_j}, a_{\lceil \frac{R_j}{2} \rceil}, a_{\lfloor \frac{R_j}{2} \rfloor} \right) \quad (49)$$

$$+ \left(2^j \left\lceil \frac{s}{2^j} \right\rceil - s \right) \cdot \psi_n \left(a_{Q_j}, a_{\lceil \frac{R_j}{2} \rceil}, a_{\lfloor \frac{R_j}{2} \rfloor} \right) = 2^j \cdot \psi_n \left(a_{Q_j}, a_{\lceil \frac{R_j}{2} \rceil}, a_{\lfloor \frac{R_j}{2} \rfloor} \right). \quad (50)$$

From (46) to (47) we upper bounded $\psi_n \left(a_{Q_j}, a_{\lceil \frac{Q_j}{2} \rceil}, a_{\lfloor \frac{Q_j}{2} \rfloor} \right)$ by $\psi_n \left(a_{Q_j}, a_{\lceil \frac{Q_j}{2} \rceil}, a_{\lfloor \frac{Q_j}{2} \rfloor} \right)$ and $\psi_n \left(a_{R_j}, a_{\lceil \frac{R_j}{2} \rceil}, a_{\lfloor \frac{R_j}{2} \rfloor} \right)$ by $\psi_n \left(a_{R_j}, a_{\lceil \frac{R_j}{2} \rceil}, a_{\lfloor \frac{R_j}{2} \rfloor} \right)$ using (38) of Lemma 2.6. We then upper bounded $\psi_n \left(a_{Q_j}, a_{\lceil \frac{Q_j}{2} \rceil}, a_{\lfloor \frac{Q_j}{2} \rfloor} \right)$ by $\psi_n \left(a_{Q_j}, a_{\lceil \frac{R_j}{2} \rceil}, a_{\lfloor \frac{R_j}{2} \rfloor} \right)$, from (47) to (48), again using (38) of Lemma 2.6. From (48) to (49), using (39) of Lemma 2.6, we bounded $\psi_n \left(a_{R_j}, a_{\lceil \frac{R_j}{2} \rceil}, a_{\lfloor \frac{R_j}{2} \rfloor} \right)$ by $\psi_n \left(a_{Q_j}, a_{\lceil \frac{R_j}{2} \rceil}, a_{\lfloor \frac{R_j}{2} \rfloor} \right)$. For the final step from (49) to (50) we factored out $\psi_n \left(a_{Q_j}, a_{\lceil \frac{R_j}{2} \rceil}, a_{\lfloor \frac{R_j}{2} \rfloor} \right)$ and then simplified.

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 (49) for $j = 0, \dots, \lceil \log_2(s) \rceil - 2$ establishing the bound of Lemma 2.7. ■

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 2.8: The problem

$$\max_{a_s, \dots, a_2} \sum_{i=1}^{\lceil s/2 \rceil} \frac{s}{2^i} \cdot \psi_n(a_{2i}, a_i, a_i) \quad (51)$$

has a global maximum and the maximum occurs at the

expected values of the a_i , \hat{a}_i given by

$$\hat{a}_{2i} = \hat{a}_i \left(2 - \frac{\hat{a}_i}{n} \right) \quad \text{for } i = 1, 2, 4, \dots, \lceil s/2 \rceil, \quad (52)$$

which are a solution of the following polynomial system.

$$\begin{aligned} a_{\lceil s/2 \rceil}^2 - 2na_{\lceil s/2 \rceil} + na_s &= 0, \\ a_{2i}^3 - 2a_i a_{2i}^2 + 2a_i^2 a_{2i} - a_i^2 a_{4i} &= 0, \end{aligned} \quad \text{for } i = 1, 2, \dots, \lceil s/4 \rceil, \quad (53)$$

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

$$a_{2i}^3 - 2a_i a_{2i}^2 + 2a_i^2 a_{2i} - a_i^2 a_{4i} = 0, \quad \text{for } i = 1, 2, 4, \dots, \lceil s/4 \rceil, \quad (54)$$

again with $a_1 = d$.

Proof: Define

$$\tilde{\Psi}_n(a_s, \dots, a_2, d) := \sum_{i=1}^{\lceil s/2 \rceil} \frac{s}{2^i} \cdot \psi_n(a_{2i}, a_i, a_i). \quad (55)$$

Using the definition of $\psi_n(\cdot)$ in (37) we therefore have

$$\begin{aligned} \tilde{\Psi}_n(a_s, \dots, a_2, d) &= \sum_{i=1}^{\lceil s/2 \rceil} \frac{s}{2^i} \cdot \left[a_i \cdot \mathbf{H} \left(\frac{a_{2i} - a_i}{a_i} \right) + \right. \\ &\quad \left. (n - a_i) \cdot \mathbf{H} \left(\frac{a_{2i} - a_i}{n - a_i} \right) - n \cdot \mathbf{H} \left(\frac{a_i}{n} \right) \right]. \end{aligned} \quad (56)$$

The gradient of $\tilde{\Psi}_n(a_s, \dots, a_2, d)$, $\nabla \tilde{\Psi}_n(a_s, \dots, a_2, d)$ is given by

$$\begin{aligned} &\left(\log \left[\frac{(2a_{\lceil s/2 \rceil} - a_s)(n - a_s)}{(a_s - a_{\lceil s/2 \rceil})^2} \right], \right. \\ &\quad \left. \frac{s}{2^i} \cdot \log \left[\frac{a_{2i}(a_{4i} - a_{2i})(2a_i - a_{2i})}{(2a_{2i} - a_{4i})(a_{2i} - a_i)^2} \right] \right)^T \\ &\quad \text{for } i = 1, 2, 4, \dots, \lceil s/4 \rceil, \end{aligned} \quad (57)$$

where v^T is the transpose of the vector v . Obtaining the critical points by solving $\nabla \tilde{\Psi}_n(a_s, \dots, a_2, d) = 0$ leads to the polynomial system (53).

The Hessian, $\nabla^2 \tilde{\Psi}_n(a_s, \dots, a_2, d)$ at these optimal a_i which are the solutions to the polynomial system (53) 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 (52) 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 joint density functions for the a_{2i} . The MLE is obtained by maximizing this summation and it corresponds to the expected log-likelihood. Therefore, the parameters given implicitly by (52) are the expected log-likelihood which implies that the values of the \hat{a}_j in (52) are the expected values of the a_i .

If we restrict a_s to take a fixed value, then $\nabla \tilde{\Psi}_n(a_s, \dots, a_2, d)$ is given by

$$\left(\frac{s}{2i} \cdot \log \left[\frac{a_{2i}(a_{4i} - a_{2i})(2a_i - a_{2i})}{(2a_{2i} - a_{4i})(a_{2i} - a_i)^2} \right] \right)^T$$

for $i = 1, 2, 4, \dots, \lceil s/4 \rceil$. (58)

Obtaining the critical points by solving $\nabla \tilde{\Psi}_n(a_s, \dots, a_2, d) = 0$ leads to the polynomial system (54).

Given a_s , the Hessian, $\nabla^2 \tilde{\Psi}_n(a_s, \dots, a_2, d)$ at these optimal a_i which are the solutions to the polynomial system (54) is negative definite which implies that this unique critical point is a global maximum; 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 $P_n(x, y, z)$ in (16); Lemma 2.10 establishes the polynomial term.

Definition 2.9: $P_n(x, y, z)$ defined in (16) satisfies the upper bound

$$P_n(x, y, z) \leq \pi(x, y, z) \exp(\psi_n(x, y, z)) \quad (59)$$

with bounds of $\pi(x, y, z)$ given in Lemma 2.10.

Lemma 2.10: For $\pi(x, y, z)$ and $P_n(x, y, z)$ given by (59) and (16) respectively, if $\{y, z\} < x < y + z$, $\pi(x, y, z)$ is given by

$$\left(\frac{5}{4} \right)^4 \left[\frac{yz(n-y)(n-z)}{2\pi n(y+z-x)(x-y)(x-z)(n-x)} \right]^{\frac{1}{2}}, \quad (60)$$

otherwise $\pi(x, y, z)$ has the following cases.

$$\left(\frac{5}{4} \right)^3 \left[\frac{y(n-z)}{n(y-z)} \right]^{\frac{1}{2}} \quad \text{if } x = y > z; \quad (61)$$

$$\left(\frac{5}{4} \right)^3 \left[\frac{(n-y)(n-z)}{n(n-y-z)} \right]^{\frac{1}{2}} \quad \text{if } x = y + z; \quad (62)$$

$$\left(\frac{5}{4} \right)^2 \left[\frac{2\pi z(n-z)}{n} \right]^{\frac{1}{2}} \quad \text{if } x = y = z. \quad (63)$$

Proof: The Stirling's inequality below would be used in this proof and other proofs to follow.

$$\begin{aligned} \frac{16}{25} (2\pi p(1-p)N)^{-\frac{1}{2}} e^{NH(p)} &\leq \binom{N}{Np} \\ &\leq \frac{5}{4} (2\pi p(1-p)N)^{-\frac{1}{2}} e^{NH(p)}, \end{aligned} \quad (64)$$

where $H(p) = -p \log(p) - (1-p) \log(1-p)$ is the Shannon entropy function for base e logarithms.

From Definition 2.9 the quantity $\pi(x, y, z)$ is the polynomial portion of the large deviation upper bound. Within this proof we express this by

$$\pi(x, y, z) = \text{poly} \left[\binom{y}{y+z-x} \binom{n-y}{x-y} \binom{n}{z}^{-1} \right]. \quad (65)$$

We derive the upper bound $\pi(x, y, z)$ using the Stirling's inequality. The right inequality of (64) is used to upper bound

$\binom{y}{y+z-x}$ and $\binom{n-y}{x-y}$ and the left inequality of (64) is used to lower bound $\binom{n}{z}$. If $\{y, z\} < x < y + z$ the bound is well defined and simplifies to (60).

If $x = y > z$ (60) is undefined; however, substituting y for x in (65) 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 (64) to bound $\binom{y}{z}$ from above and the left inequality in (64) to bound from below $\binom{n}{z}$. The resulting polynomial part of the product simplifies to (61).

If $x = y + z$, then $\binom{y}{y+z-x} = \binom{y}{0} = 1$ and $\binom{n-y}{x-y} = \binom{n-y}{n-y} = 1$. As above, we upper bound the product of $\binom{n-y}{x-y}$ and $\binom{n}{z}^{-1}$ using (64) and simplify the polynomial part of this product to get (62). If instead $x = y = z$, then $\binom{y}{y+z-x} = \binom{y}{0} = 1$ and $\binom{n-y}{x-y} = \binom{n-y}{0} = 1$ both of which equal 1. Therefore the bound only involves $\binom{n}{z}^{-1}$ which we bound using (64) and the resulting polynomial part simplifies to (63). ■

Corollary 2.11: If $n > 2y$, then $\pi(y, y, y)$ is monotonically increasing in y .

Proof: If $n > 2y$, (63) 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 . ■

III. RESTRICTED ISOMETRY CONSTANTS AND COMPRESSED SENSING ALGORITHMS

Here we introduce RIC_2 and briefly discuss the implications of RIC_1 and RIC_2 to compressed sensing algorithms in Section III-A. In Section III-B we present the first ever quantitative comparison of the performance guarantees of some of the compressed sensing algorithms proposed for sparse matrices as stated in Definition 1.3.

A. Restricted isometry constants

It is possible to include noise in the Compressed Sensing model, for instance $y = Ax + e$ where e is a noise vector capturing the model misfit or the non-sparsity of the signal x . The ℓ_0 -minimization problem (7) in the noise case setting is

$$\min_{x \in \mathcal{X}^N} \|x\|_0 \quad \text{subject to} \quad \|Ax - y\|_2 < \|e\|_2, \quad (66)$$

where $\|e\|_2$ is the magnitude of the noise.

Problems (7) and (66) are in general NP-hard and hence intractable. To benefit from the rich literature of algorithms available in both convex and non-convex optimization the ℓ_0 -minimization problem is relaxed to an ℓ_p -minimization one for $0 < p \leq 1$. It is well known that the ℓ_p norm for $0 < p \leq 1$ are sparsifying norms, see [19], [21]. In addition, there are specifically designed classes of algorithms that take on the ℓ_0 problem and they have been referred to as greedy algorithms. When using dense sensing matrices, A , popular greedy algorithms include Normalized Iterative Hard Thresholding (NIHT), [26], Compressive Sampling Matching Pursuits (CoSAMP), [22], and Subspace Pursuit (SP), [20]. When A is sparse and non-mean zero, a different set of *combinatorial* greedy algorithms have been proposed which iteratively locates and eliminate large (in magnitude) components of the vector, [5]. They include Expander Matching

Pursuit (EMP), [27], Sparse Matching Pursuit (SMP), [28], Sequential Sparse Matching Pursuit (SSMP), [29], Left Degree Dependent Signal Recovery (LDDSR), [24], and Expander Recovery (ER), [23], [7].

The convergence analysis of nearly all of these algorithms rely heavily on restricted isometry constants (RIC). As we saw earlier RICs measures how near isometry A is when applied to k -sparse vectors in some norm. For the ℓ_1 norm, also known as the Manhattan norm, RIC_1 is stated in (8). The restricted Euclidian norm isometry, introduced by Candès in [30], is denoted by RIC_2 and is defined in Definition 3.1.

Definition 3.1 (RIC_2): Define χ^N to be the set of all k -sparse vectors and draw an $n \times N$ matrix A , then for all $x \in \chi^N$, A has RIC_2 , with lower and upper RIC_2 , $L(k, n, N; A)$ and $U(k, n, N; A)$ respectively, when the following holds.

$$(1 - L(k, n, N; A)) \|x\|_2 \leq \|Ax\|_2 \\ \leq (1 + U(k, n, N; A)) \|x\|_2.$$

The computation of RIC_1 for adjacency matrices of lossless (k, d, ϵ) -expander graphs is equivalent to calculating ϵ . The computation of RIC_2 is intractable except for trivially small problem sizes (k, n, N) because it involves doing a combinatorial search over all $\binom{N}{k}$ column submatrices of A . As a results attempts have been made to derive RIC_2 bounds. Some of these attempts have been successful in deriving RIC_2 bounds for the Gaussian ensemble and these bounds have evolved from the first by Candès and Tao in [19], improved by Blanchard, Cartis and Tanner in [31] and further improved by Bah and Tanner in [32].

RIC_2 bounds have been used to derive sampling theorems for compressed sensing algorithms - ℓ_1 -minimization and the greedy algorithms for dense matrices, NIHT, CoSAMP, and SP. Using the phase transition framework with RIC_2 bounds Blanchard et. al. compared performance of these algorithms in [13]. In a similar vain, as another key contribution of this paper we provide sampling theorems for ℓ_1 -minimization and combinatorial greedy algorithms, EMP, SMP, SSMP, LDDSR and ER, proposed for SE and SSE matrices.

B. Algorithms and their performance guarantees

Theoretical guarantees have been given for ℓ_1 recovery and 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 ℓ_1 -minimization and some of the aforesaid algorithms, see [5], [6], [23], [4], [24] and the references therein. Base on theoretical guarantees, we derived sampling theorems and present here phase transition curves which are plots of phase transition functions $\rho^{\text{alg}}(\delta; d, \epsilon)$ of algorithms such that for $k/n \rightarrow \rho < (1 - \gamma)\rho^{\text{alg}}(\delta; d, \epsilon)$, $\gamma > 0$, a given algorithm is guaranteed to recovery all k -sparse signals with overwhelming probability approaching one exponentially in n .

1) ℓ_1 -minimization: Note that ℓ_1 -minimization is not an algorithm per se, but can be solved using Linear Programming (LP) algorithms. Berinde et. al. showed in [5] that ℓ_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 [5], [6].

Theorem 3.2 (*Theorem 3*, [5], *Theorem 1*, [6]): Let A be an adjacency matrix of a lossless (k, d, ϵ) -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

$$\|x - \hat{x}\|_1 \leq \frac{2}{1 - 2\alpha(\epsilon)} \|x - x_k\|_1. \quad (67)$$

The condition that $\alpha(\epsilon) = 2\epsilon/(1 - 2\epsilon) < 1/2$ implies the sampling theorem stated as Corollary 3.3, that when satisfied ensures a positive upper bound in (67). The resulting sampling theorem is given by $\rho^{\ell_1}(\delta; d, \epsilon)$ using $\epsilon = 1/6$ from Corollary 3.3.

Corollary 3.3 ([5]): ℓ_1 -minimization is guaranteed to recover any k -sparse vector from its linear measurement by an adjacency matrix of a lossless (k, d, ϵ) -expander graph with $\epsilon < 1/6$.

Proof: Setting the denominator of the fraction in the right hand side of (67) to be greater than zero gives the required results. ■

2) *Sequential Sparse Matching Pursuit (SSMP)*: Introduced by Indyk and Ruzic in [29], 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 [27] uses a voting-like mechanism to identify and eliminate large (in magnitude) components of 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 [28], improved on the drawback of EMP. However, it's original version had convergence problems when the input parameters (k and n) fall outside the theoretically guaranteed region. This is fixed by 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 parallel, consequently convergence is automatically achieved. All three algorithms have the same theoretical recovery guarantees, which we state in Theorem 3.4, but SSMP has better empirical performances compared to it's predecessors.

Algorithm 1 below 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 , $L((c + 1)k, n, N) = \epsilon$. The measurement vector $y = Ax + e$ where e is a noise vector and $\eta = \|e\|_1$. We denote by $H_k(y)$ the hard thresholding operator which sets to zero all but the largest, in magnitude, k entries of y .

The recovery guarantees for SSMP (also for EMP and SMP) are formalized by the following theorem from which

Algorithm 1 Sequential Sparse Matching Pursuit (SSMP) [29]**Input:** A, y, η **Output:** k -sparse approximation \hat{x} of the target signal x **Initialization:**

1. Set $j = 0$
2. Set $x_j = 0$

Iteration: Repeat $T = \mathcal{O}(\log(\|x\|_1/\eta))$ times

1. Set $j = j + 1$
2. Repeat $(c - 1)k$ times
 - a) Find a coordinate i & an increment z that minimizes $\|A(x_j + ze_i) - y\|_1$
 - b) Set x_j to $x_j + ze_i$
3. Set $x_j = H_k(x_j)$

Return $\hat{x} = x^T$

we deduce the recovery condition (sampling theorem) in terms of ϵ in Corollary 3.5. Based on Corollary 3.5 deduced from Theorem 3.4 we derived phase transition, $\rho^{SSMP}(\delta; d, \epsilon)$, for SSMP.

Theorem 3.4 (Theorem 10, [27]): Let A be an adjacency matrix of a lossless (k, d, ϵ) -expander graph with $\epsilon < 1/16$. Given a vector $y = Ax + e$, the algorithm returns approximation vector \hat{x} satisfying

$$\|x - \hat{x}\|_1 \leq \frac{1 - 4\epsilon}{1 - 16\epsilon} \|x - x_k\|_1 + \frac{6}{(1 - 16\epsilon)d} \|e\|_1, \quad (68)$$

where x_k is the k largest (in magnitude) coordinates of x .

Corollary 3.5 ([27]): 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, ϵ) -expander graph with $\epsilon < 1/16$.

3) *Expander Recovery (ER):* Introduced by Jafarpour et al. in [23], [7], ER is an improvement on an earlier algorithm introduced by Xu and Hassibi in [24] 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, ϵ) -expander for any $\epsilon < 1/4$ for ER. Both algorithms use this concept of a *gap* defined below.

Definition 3.6 (gap, [24], [23], [7]): 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:

$$g_i = y_i - \sum_{j=1}^N A_{ij} \hat{x}_j. \quad (69)$$

Algorithm 2 below 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 [23], [7] have a modified version of the algorithm for when x is almost k -sparse.

Theorem 3.7 gives recovery guarantees for ER. Directly from this theorem we read-off the recovery condition in terms of ϵ for Corollary 3.8, from which we derive phase transition functions, $\rho^{ER}(\delta; d, \epsilon)$, for ER.

Theorem 3.7 (Theorem 6, [7]): Let $A \in \mathbb{R}^{n \times N}$ be the adjacency matrix of a lossless $(2k, d, \epsilon)$ -expander graph, where $\epsilon < 1/4$ and $n = \mathcal{O}(k \log(N/k))$. Then, for any k -sparse

Algorithm 2 Expander Recovery (ER) [23], [7]**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
5. Set $\hat{x}_j = \hat{x}_j + g$, and go to 2.
6. **end if**

signal x , given $y = Ax$, ER recovers x successfully in at most $2k$ iterations.

Corollary 3.8: ER is guaranteed to recover any k -sparse vector from its linear measurement by an adjacency matrix of a lossless (k, d, ϵ) -expander graph with $\epsilon < 1/4$.

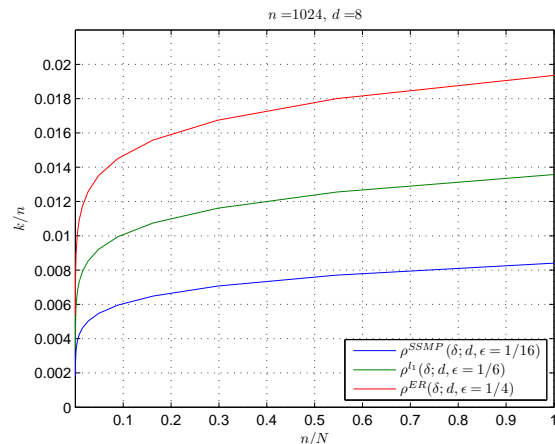


Fig. 10. Phase transition curves $\rho^{alg}(\delta; d, \epsilon)$ computed over finite values of $\delta \in (0, 1)$ with d fixed and the different ϵ values for each algorithm - 1/4, 1/6 and 1/16 for ER, ℓ_1 and SSMP respectively.

4) *Comparisons of phase transitions of algorithms:* Figure 10 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 ℓ_1 -minimization. Remarkably, for ER and LDDSR recovery is guaranteed for a larger portion of the (δ, ρ) plane than is guaranteed by the theory for ℓ_1 -minimization using sparse matrices; however, ℓ_1 -minimization has a larger recovery region than does SSMP, EMP, and SMP.

Figure 11 shows a comparison of the phase transition of ℓ_1 -minimization as presented by Blanchard et al. in [13] 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 RIC_1 being more closely related to ℓ_1 -minimization than is RIC_2 .

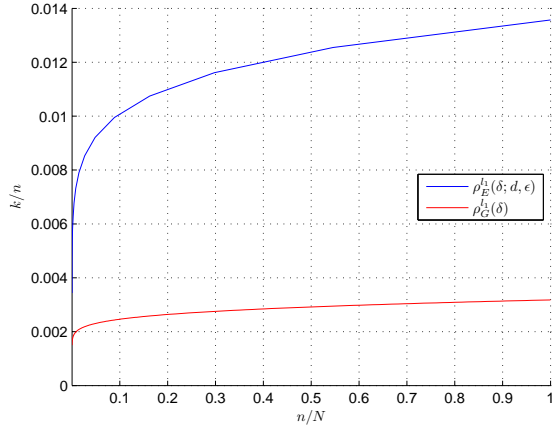


Fig. 11. Phase transition plots of l_1 , $\rho_G^{\ell_1}(\delta)$, for Gaussian matrices derived using RIC₂ and $\rho_E^{\ell_1}(\delta; d, \epsilon)$ for adjacency matrices of expander graphs with $n = 1024$, $d = 8$, and $\epsilon = 1/6$.

IV. PROOF OF MAINS RESULTS

A. Proof of Theorem 1.6

By the dyadic splitting $|A_s| = \left| A_{\lceil \frac{s}{2} \rceil}^1 \cup A_{\lfloor \frac{s}{2} \rfloor}^2 \right|$ and therefore

$$\text{Prob}(|A_s| \leq a_s) = \text{Prob}\left(\left| A_{\lceil \frac{s}{2} \rceil}^1 \cup A_{\lfloor \frac{s}{2} \rfloor}^2 \right| \leq a_s\right) \quad (70)$$

$$= \sum_{l_s} \sum_{l_{\lceil \frac{s}{2} \rceil}, l_{\lfloor \frac{s}{2} \rfloor}} \text{Prob}\left(\left| A_{\lceil \frac{s}{2} \rceil}^1 \cup A_{\lfloor \frac{s}{2} \rfloor}^2 \right| = l_s\right) \quad (71)$$

$$= \sum_{l_s} \sum_{l_{\lceil \frac{s}{2} \rceil}^1} \sum_{l_{\lfloor \frac{s}{2} \rfloor}^2} \text{P}_n\left(l_s, l_{\lceil \frac{s}{2} \rceil}^1, l_{\lfloor \frac{s}{2} \rfloor}^2\right) \times \text{Prob}\left(\left| A_{\lceil \frac{s}{2} \rceil}^1 \right| = l_{\lceil \frac{s}{2} \rceil}^1\right) \text{Prob}\left(\left| A_{\lfloor \frac{s}{2} \rfloor}^2 \right| = l_{\lfloor \frac{s}{2} \rfloor}^2\right). \quad (72)$$

From (70) to (71) we sum over all possible events while from (71) to (72), in line with the splitting technique, we simplify the probability to the product of the probabilities of the cardinalities of $\left| A_{\lceil \frac{s}{2} \rceil}^1 \right|$ and $\left| A_{\lfloor \frac{s}{2} \rfloor}^2 \right|$ and their intersection.

In a slight abuse of notation we write $\sum^{l^j}_{j=1, \dots, x}$ to denote applying the sum x times. Now we use Lemma 2.5 to simplify (72) as follows.

$$\sum_{j_1=1, \dots, q_0} \sum_{j_2=1, \dots, q_1} \sum_{j_3=1, \dots, r_1} \text{P}_n\left(l_{Q_0}^{j_1}, l_{\lceil \frac{Q_0}{2} \rceil}^{2j_1-1}, l_{\lfloor \frac{Q_0}{2} \rfloor}^{2j_1}\right) \times \prod_{j_2=1}^{q_1} \text{Prob}\left(\left| A_{Q_1}^{j_2} \right| = l_{Q_1}^{j_2}\right) \times \prod_{j_3=q_1+1}^{q_1+r_1} \text{Prob}\left(\left| A_{R_1}^{j_3} \right| = l_{R_1}^{j_3}\right). \quad (73)$$

Let's quickly verify that (73) is the same as (72). By Lemma 2.5, $Q_0 = s$ 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 $\text{P}_n(\cdot)$ 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 (72) i.e. the second two summations and the product of the two $\text{Prob}(\cdot)$.

Now we proceed with the splitting - note (73) 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.

$$\sum_{j_1=1, \dots, q_0} \sum_{j_2=1, \dots, q_1} \sum_{j_3=1, \dots, r_1} \text{P}_n\left(l_{Q_0}^{j_1}, l_{\lceil \frac{Q_0}{2} \rceil}^{2j_1-1}, l_{\lfloor \frac{Q_0}{2} \rfloor}^{2j_1}\right) \times \left[\sum_{j_4=1, \dots, q_2} \sum_{j_5=1, \dots, r_2} \text{P}_n\left(l_{Q_1}^{j_2}, l_{\lceil \frac{Q_1}{2} \rceil}^{2j_2-1}, l_{\lfloor \frac{Q_1}{2} \rfloor}^{2j_2}\right) \text{P}_n\left(l_{R_1}^{j_3}, l_{\lceil \frac{R_1}{2} \rceil}^{2j_3-1}, l_{\lfloor \frac{R_1}{2} \rfloor}^{2j_3}\right) \times \prod_{j_4=1}^{q_2} \text{Prob}\left(\left| A_{Q_1}^{j_4} \right| = l_{Q_1}^{j_4}\right) \prod_{j_5=q_2+1}^{q_2+r_2} \text{Prob}\left(\left| A_{R_1}^{j_5} \right| = l_{R_1}^{j_5}\right) \right]. \quad (74)$$

We continue this splitting of each instance of $\text{Prob}(\cdot)$ 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 $\text{P}_n(\cdot)$ which we express as

$$\sum_{j_1=1, \dots, q_0} \sum_{j_2=1, \dots, q_1} \sum_{j_3=1, \dots, r_1} \text{P}_n\left(l_{Q_0}^{j_1}, l_{\lceil \frac{Q_0}{2} \rceil}^{2j_1-1}, l_{\lfloor \frac{Q_0}{2} \rfloor}^{2j_1}\right) \times \left[\sum_{j_4=1, \dots, q_2} \sum_{j_5=1, \dots, r_2} \text{P}_n\left(l_{Q_1}^{j_2}, l_{\lceil \frac{Q_1}{2} \rceil}^{2j_2-1}, l_{\lfloor \frac{Q_1}{2} \rfloor}^{2j_2}\right) \times \text{P}_n\left(l_{R_1}^{j_3}, l_{\lceil \frac{R_1}{2} \rceil}^{2j_3-1}, l_{\lfloor \frac{R_1}{2} \rfloor}^{2j_3}\right) \cdot \left[\dots \left[\sum_{j_2 \lceil \log_2 s \rceil - 2}^{j_2 \lceil \log_2 s \rceil - 1} l_{Q \lceil \log_2 s \rceil - 1}^{j_2} \text{P}_n\left(l_4^{j_2 \lceil \log_2 s \rceil - 4}, l_2^{2j_2 \lceil \log_2 s \rceil - 4 - 1}, l_2^{2j_2 \lceil \log_2 s \rceil - 4}\right) \times \text{P}_n\left(l_3^{j_2 \lceil \log_2 s \rceil - 3}, l_2^{2j_2 \lceil \log_2 s \rceil - 3 - 1}, d\right) \times \text{P}_n\left(l_2^{j_2 \lceil \log_2 s \rceil - 2}, d, d\right) \right] \dots \right]. \quad (75)$$

Using the definition of $\text{P}_n(\cdot)$ in Lemma 2.3 we bound (75) by bounding each $\text{P}_n(\cdot)$ as in (59) with a product of

a polynomial, $\pi(\cdot)$, and an exponential with exponent $\psi_n(\cdot)$.

$$\begin{aligned}
& \sum_{l_{Q_0}^{j_1}} \sum_{l_{Q_1}^{j_2}} \sum_{l_{R_1}^{j_3}} \pi \left(l_{Q_0}^{j_1}, l_{\lceil \frac{Q_0}{2} \rceil}^{2j_1-1}, l_{\lfloor \frac{Q_0}{2} \rfloor}^{2j_1} \right) \times \\
& e^{\psi_n \left(l_{Q_0}^{j_1}, l_{\lceil \frac{Q_0}{2} \rceil}^{2j_1-1}, l_{\lfloor \frac{Q_0}{2} \rfloor}^{2j_1} \right)} \cdot \left[\sum_{l_{Q_2}^{j_4}} \sum_{l_{R_2}^{j_5}} \right. \\
& \pi \left(l_{Q_1}^{j_2}, l_{\lceil \frac{Q_1}{2} \rceil}^{2j_2-1}, l_{\lfloor \frac{Q_1}{2} \rfloor}^{2j_2} \right) \cdot e^{\psi_n \left(l_{Q_1}^{j_2}, l_{\lceil \frac{Q_1}{2} \rceil}^{2j_2-1}, l_{\lfloor \frac{Q_1}{2} \rfloor}^{2j_2} \right)} \times \\
& \pi \left(l_{R_1}^{j_3}, l_{\lceil \frac{R_1}{2} \rceil}^{2j_3-1}, l_{\lfloor \frac{R_1}{2} \rfloor}^{2j_3} \right) \cdot e^{\psi_n \left(l_{R_1}^{j_3}, l_{\lceil \frac{R_1}{2} \rceil}^{2j_3-1}, l_{\lfloor \frac{R_1}{2} \rfloor}^{2j_3} \right)} \\
& \times \left[\dots \times \left[\sum_{l_{Q_{\lceil \log_2 s \rceil - 1}}^{j_{2\lceil \log_2 s \rceil - 2}}} \right. \right. \\
& \pi \left(l_4^{j_2\lceil \log_2 s \rceil - 4}, l_2^{2j_2\lceil \log_2 s \rceil - 4 - 1}, l_2^{2j_2\lceil \log_2 s \rceil - 4} \right) \\
& \times e^{\psi_n \left(l_4^{j_2\lceil \log_2 s \rceil - 4}, l_2^{2j_2\lceil \log_2 s \rceil - 4 - 1}, l_2^{2j_2\lceil \log_2 s \rceil - 4} \right)} \\
& \times \pi \left(l_3^{j_2\lceil \log_2 s \rceil - 3}, l_2^{2j_2\lceil \log_2 s \rceil - 3 - 1}, d \right) \\
& \times e^{\psi_n \left(l_3^{j_2\lceil \log_2 s \rceil - 3}, l_2^{2j_2\lceil \log_2 s \rceil - 3 - 1}, d \right)} \times \\
& \left. \left. \pi \left(l_2^{j_2\lceil \log_2 s \rceil - 2}, d, d \right) \cdot e^{\psi_n \left(l_2^{j_2\lceil \log_2 s \rceil - 2}, d, d \right)} \right] \dots \right]. \quad (76)
\end{aligned}$$

Using Lemma 2.6 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 $\Psi_n(a_s, \dots, a_2, d)$. The factor involving the $\pi(\cdot)$ will be called $\Pi(l_s, \dots, l_2, d)$ and we have the following upper bound for (76).

$$\Pi(l_s, \dots, l_2, d) \cdot \exp[\Psi_n(a_s, \dots, a_2, d)], \quad (77)$$

where the exponent $\Psi_n(a_s, \dots, a_2, d)$ is given by

$$\psi_n \left(a_{Q_0}, a_{\lceil \frac{Q_0}{2} \rceil}, a_{\lfloor \frac{Q_0}{2} \rfloor} \right) + \dots + \psi_n(a_2, d, d). \quad (78)$$

Now we attempt to bound the probability of interest in (70). This task reduces to bounding $\Pi(l_s, \dots, l_2, d)$ and $\Psi_n(a_s, \dots, a_2, d)$ in (77) and we start with the former, i.e. bounding $\Pi(l_s, \dots, l_2, d)$. We bound each sum of $\pi(\cdot)$ in $\Pi(l_s, \dots, l_2, d)$ of (77) by the maximum of summations multiplied by the number of terms in the sum. From (63) we see that $\pi(\cdot)$ is maximized when all the three arguments are the same and using Corollary 2.11 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 4.1: 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 maximum 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 2.5 give the following upper bound on $\Pi(l_s, \dots, l_2, d)$.

$$\begin{aligned}
& \left(\left\lceil \frac{Q_0}{2} \right\rceil d \left(\frac{5}{4} \right)^2 \sqrt{2\pi \left\lceil \frac{Q_0}{2} \right\rceil d} \right)^{q_0} \times \\
& \prod_{j=1}^{\lceil \log_2 s \rceil - 2} \left[\left(\left\lceil \frac{Q_j}{2} \right\rceil d \left(\frac{5}{4} \right)^2 \sqrt{2\pi \left\lceil \frac{Q_j}{2} \right\rceil d} \right)^{q_j} \times \right. \\
& \left. \left(\left\lceil \frac{R_j}{2} \right\rceil d \left(\frac{5}{4} \right)^2 \sqrt{2\pi \left\lceil \frac{R_j}{2} \right\rceil d} \right)^{r_j} \right] \times \\
& \left(\left\lceil \frac{Q_{\lceil \log_2 s \rceil - 1}}{2} \right\rceil d \left(\frac{5}{4} \right)^2 \sqrt{2\pi \left\lceil \frac{Q_{\lceil \log_2 s \rceil - 1}}{2} \right\rceil d} \right)^{q_{\lceil \log_2 s \rceil - 1}} \quad (79)
\end{aligned}$$

Proof: From (63) we have

$$\pi(y, y, y) = \left(\frac{5}{4} \right)^2 \sqrt{\frac{2\pi y(n-y)}{n}} < \left(\frac{5}{4} \right)^2 \sqrt{2\pi y}. \quad (80)$$

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 $x \geq y \geq z$. 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 $l_{\lfloor \frac{Q_j}{2} \rfloor}$ is $\lfloor \frac{Q_j}{2} \rfloor \cdot d$ since there are d nonzeros in each column. Also $l_{\lfloor \frac{Q_j}{2} \rfloor} \leq l_{Q_j} \leq l_{\lfloor \frac{Q_j}{2} \rfloor} + l_{\lceil \frac{Q_j}{2} \rceil}$ so the number of terms in the summation over l_{Q_j} is $\lceil \frac{Q_j}{2} \rceil \cdot d$, 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 2.5.

We replace y by $\lfloor \frac{Q_j}{2} \rfloor \cdot d$ or $\lceil \frac{R_j}{2} \rceil \cdot d$ accordingly into the bound of $\pi(y, y, y)$ in (80) and multiply by the number of terms in the summation, i.e. $\lceil \frac{Q_j}{2} \rceil \cdot d$ or $\lceil \frac{R_j}{2} \rceil \cdot d$. 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 (79) hence concluding the proof of Proposition 4.1. ■

As a final step we need the following corollary.

Corollary 4.2:

$$\Pi(l_s, \dots, l_2, d) < \frac{2}{25\sqrt{2\pi s^3 d^3}} \cdot \exp[3s \log(5d)]. \quad (81)$$

Proof:

From Lemma 2.5 we can upper bound R_j by Q_j . Conse-

quently (79) is upper bounded by the following.

$$\begin{aligned} & \left(\left\lceil \frac{Q_0}{2} \right\rceil d \left(\frac{5}{4} \right)^2 \sqrt{2\pi \left\lceil \frac{Q_0}{2} \right\rceil d} \right)^{q_0} \times \\ & \prod_{j=1}^{\lceil \log_2 s \rceil - 2} \left(\left\lceil \frac{Q_j}{2} \right\rceil d \left(\frac{5}{4} \right)^2 \sqrt{2\pi \left\lceil \frac{Q_j}{2} \right\rceil d} \right)^{q_j + r_j} \times \\ & \left(\left\lceil \frac{Q_{\lceil \log_2 s \rceil - 1}}{2} \right\rceil d \left(\frac{5}{4} \right)^2 \sqrt{2\pi \left\lceil \frac{Q_{\lceil \log_2 s \rceil - 1}}{2} \right\rceil d} \right)^{q_{\lceil \log_2 s \rceil - 1}} \end{aligned} \quad (82)$$

Now we use the property that $q_j + r_j = 2^j$ for $j = 1, \dots, \lceil \log_2 s \rceil - 1$ from Lemma 2.5 to bound (82) by the following.

$$\prod_{j=0}^{\lceil \log_2 s \rceil - 1} \left(\left\lceil \frac{Q_j}{2} \right\rceil d \left(\frac{5}{4} \right)^2 \sqrt{2\pi \left\lceil \frac{Q_j}{2} \right\rceil d} \right)^{2^j}. \quad (83)$$

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 (83) 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 2.5. Thus $\left\lceil \frac{Q_j}{2} \right\rceil = \left\lceil \frac{s}{2^{j+1}} \right\rceil$ and $\left\lceil \frac{Q_j}{2} \right\rceil \leq \left\lceil \frac{s}{2^{j+1}} \right\rceil$. So we bound (83) by the following.

$$\prod_{j=0}^{\lceil \log_2 s \rceil - 1} \left(\left\lceil \frac{s}{2^{j+1}} \right\rceil d \left(\frac{5}{4} \right)^2 \sqrt{2\pi \left\lceil \frac{s}{2^{j+1}} \right\rceil d} \right)^{2^j} \quad (84)$$

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 (84).

$$\begin{aligned} & \prod_{j=0}^{\log_2 s} \left[\frac{s}{2^{j+1}} \left(1 + \frac{2^{j+1}}{s} \right) \left(\frac{25\sqrt{2\pi}}{16} \right) \times \right. \\ & \left. \sqrt{\frac{s}{2^{j+1}} \left(1 + \frac{2^{j+1}}{s} \right) d^3} \right]^{2^j}. \end{aligned}$$

We bound $\left(1 + \frac{2^{j+1}}{s} \right)$ by 2 to bound the above by

$$\begin{aligned} & \prod_{j=0}^{\log_2 s} \left[\frac{s}{2^j} \left(\frac{25\sqrt{2\pi}}{16} \right) \sqrt{\frac{s}{2^j} d^3} \right]^{2^j} \\ & = \prod_{j=0}^{\log_2 s} \left[\left(\frac{25\sqrt{2\pi}}{16} \right) \sqrt{\frac{s^3 d^3}{2^{3j}}} \right]^{2^j} \end{aligned} \quad (85)$$

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.

$$\left(\frac{25\sqrt{2\pi}}{16} \right)^{\sum_{i=0}^{\log_2 s} 2^i} \left[\prod_{j=0}^{\log_2 s} \left(\frac{sd}{2^j} \right)^{2^j} \right]^{3/2} \quad (86)$$

$$= \left(\frac{25\sqrt{2\pi}}{16} \right)^{2^{s-1}} \left[(sd)^{\sum_{i=0}^{\log_2 s} 2^i} \prod_{j=0}^{\log_2 s} \left(\frac{1}{2^j} \right)^{2^j} \right]^{3/2} \quad (87)$$

$$= \left(\frac{25\sqrt{2\pi}}{16} \right)^{2^{s-1}} \left[(sd)^{2^{s-1}} \left(\frac{1}{2} \right)^{\sum_{j=0}^{\log_2 s} j 2^j} \right]^{3/2}. \quad (88)$$

From (86) to (87) 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 (87) to (88) 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.

$$\sum_{k=1}^m k \cdot 2^k = (m-1) \cdot 2^{m+1} + 2. \quad (89)$$

This therefore simplifies (88) as follows.

$$\left(\frac{25\sqrt{2\pi}}{16} \right)^{2^{s-1}} \left[(sd)^{2^{s-1}} \left(\frac{1}{2} \right)^{(\log_2 s - 1) \cdot 2^{\log_2 s + 1} + 2} \right]^{3/2} \quad (90)$$

$$= \left(\frac{25\sqrt{2\pi}}{16} \right)^{2^{s-1}} \left[(sd)^{2^{s-1}} \left(\frac{1}{2} \right)^{2s(\log_2 s - 1)} \frac{1}{4} \right]^{3/2} \quad (91)$$

$$= \left(\frac{25\sqrt{2\pi}}{16} \right)^{2^{s-1}} \left[\frac{(sd)^{2s}}{4sd} 2^{-2s \log_2 s} s^{2s} \right]^{3/2} \quad (92)$$

$$= \left(\frac{25\sqrt{2\pi}}{16} \right)^{2^s} \left(\frac{16}{25\sqrt{2\pi}} \right) \left[\frac{(2sd)^{2s}}{4sd} s^{-2s} \right]^{3/2} \quad (93)$$

$$= \left(\frac{25\sqrt{2\pi}}{16} \right)^{2^s} \left(\frac{16}{25\sqrt{2\pi}} \right) \left[\frac{(2d)^{2s}}{4sd} \right]^{3/2}. \quad (94)$$

From (90) through (92) we simplified using basic properties of indices and logarithms. While from (92) to (93) we incorporated 2^{2s} into the first factor inside the square brackets and we rewrote the first factor into a product of a power in s and another without s . From (93) to (94) the s^{2s} and s^{-2s} canceled out.

Now we expand the square brackets in (94) to have (95) below.

$$\left(\frac{25\sqrt{2\pi}}{16}\right)^{2s} \left(\frac{16}{25\sqrt{2\pi}}\right) \frac{1}{8\sqrt{s^3 d^3}} (2d)^{3s} \quad (95)$$

$$= \left(\frac{25\sqrt{2\pi}}{16}\right)^{2s} (2d)^{3s} \frac{2}{25\sqrt{2\pi s^3 d^3}} \quad (96)$$

$$= \frac{2}{25\sqrt{2\pi s^3 d^3}} \cdot \exp\left(3s \log\left(2\left(\frac{25\sqrt{2\pi}}{16}\right)^{2/3} d\right)\right) \quad (97)$$

$$< \frac{2}{25\sqrt{2\pi s^3 d^3}} \cdot \exp[3s \log(5d)] \quad (98)$$

From (95) to (96) we simplified and from (96) to (97) we rewrote the powers as an exponential with a logarithmic exponent. Then from (97) to (98) we upper bounded $2\left(\frac{25\sqrt{2\pi}}{16}\right)^{2/3}$ 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 4.2 we have completed the bounding of $\Pi(l_s, \dots, l_2, d)$ in (77). Next we bound $\Psi_n(a_s, \dots, a_2, d)$ which is given by (78). Lemma 2.5 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 $\Psi_n(a_s, \dots, a_2, d)$ as

$$\sum_{j=0}^{\lceil \log_2(s) \rceil - 2} \left[q_j \cdot \psi_n\left(a_{Q_j}, a_{\lfloor \frac{Q_j}{2} \rfloor}, a_{\lfloor \frac{Q_j}{2} \rfloor}\right) + r_j \cdot \psi_n\left(a_{R_j}, a_{\lfloor \frac{R_j}{2} \rfloor}, a_{\lfloor \frac{R_j}{2} \rfloor}\right) \right] + q_{\lceil \log_2(s) \rceil - 1} \cdot \psi_n(a_2, d, d). \quad (99)$$

Equation (99) is bounded above in Lemma 2.7 by the following.

$$\sum_{j=0}^{\lceil \log_2(s) \rceil - 1} 2^j \cdot \psi_n\left(a_{Q_j}, a_{\lfloor \frac{R_j}{2} \rfloor}, a_{\lfloor \frac{R_j}{2} \rfloor}\right). \quad (100)$$

If we let the $a_{2i} = a_{Q_j}$ and $a_i = a_{\lfloor \frac{R_j}{2} \rfloor}$ we have (100) equal to the following.

$$\sum_{i=1}^{\lceil s/2 \rceil} \frac{s}{2i} \cdot \psi_n(a_{2i}, a_i, a_i) = \sum_{i=1}^{\lceil s/2 \rceil} \frac{s}{2i} \left[a_i \cdot \mathbf{H}\left(\frac{a_{2i} - a_i}{a_i}\right) + (n - a_i) \cdot \mathbf{H}\left(\frac{a_{2i} - a_i}{n - a_i}\right) - n \cdot \mathbf{H}\left(\frac{a_i}{n}\right) \right]. \quad (101)$$

Now we combine the bound of $\Pi(l_s, \dots, l_2, d)$ in (81) and the exponential whose exponent is the bound of $\Psi_n(a_s, \dots, a_2, d)$ in (101) to get (2), the polynomial $p_{max}(s, d) = \frac{2}{25\sqrt{2\pi s^3 d^3}}$, and (3), the exponent of the exponential $\Psi(a_s, \dots, d)$ which is given by the sum of $3s \log(5d)$ and the right hand side of (101).

Lemma 2.8 gives the a_i that maximize (101) and the systems (53) and (54) they satisfy depending on the constraints on a_s . Solving completely the system (53) gives \hat{a}_i in (52) and (4) which are the expected values of the a_i . The system (5) is equivalent to (54) hence also proven in Lemma 2.8. This therefore concludes the proof Theorem 1.6.

B. Main Corollaries

In this section we present the proofs of the corollaries in Sections I-A and I-B. These include the proof of Corollary 1.7 in Section IV-B1, the proof of Corollary 1.10 in Section IV-B2 and the proof of Corollary 1.11 given in Section IV-B3.

1) *Corollary 1.7:* Satisfying RIP-1 means that for any s -sparse vector x , $\|A_S x\|_1 \geq (1 - 2\epsilon)d\|x\|_1$ which indicates that the cardinality of the set of neighbors satisfies $|A_s| \geq (1 - \epsilon)ds$. Therefore

$$\begin{aligned} \text{Prob}(\|A_S x\|_1 \leq (1 - 2\epsilon)d\|x\|_1) \\ \equiv \text{Prob}(|A_s| \leq (1 - \epsilon)ds). \end{aligned} \quad (102)$$

This implies that $a_s = (1 - \epsilon)ds$ and since this is restricting a_s to be less than it's expected value given by (4), the rest of the a_i satisfy the polynomial system (5). If there exists a solution then the a_i would be functions of s , d and ϵ which makes $\Psi(a_s, \dots, a_2, d) = \Psi(s, d, \epsilon)$.

2) *Corollary 1.10:* Corollary 1.7 states that by fixing S and the other parameters, $\text{Prob}(\|A_S x\|_1 \leq (1 - 2\epsilon)d\|x\|_1) < p_{max}(s, d) \cdot \exp[n \cdot \Psi(s, d, \epsilon)]$. Corollary 1.10 considers any $S \subset [N]$ and since the matrices are adjacency matrices of lossless expanders we need to consider any $S \subset [N]$ such that $|S| \leq k$. Therefore our target is $\text{Prob}(\|Ax\|_1 \leq (1 - 2\epsilon)d\|x\|_1)$ 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.

$$\sum_{s=2}^k \binom{N}{s} \cdot \text{Prob}(\|A_S x\|_1 \leq (1 - 2\epsilon)d\|x\|_1) \quad (103)$$

$$< \sum_{s=2}^k \binom{N}{s} \cdot p_{max}(s, d) \cdot \exp[n \cdot \Psi(s, d, \epsilon)] \quad (104)$$

$$< \sum_{s=2}^k \left(\frac{5}{4}\right)^2 \frac{1}{\sqrt{2\pi s(1 - \frac{s}{N})}} \cdot p_{max}(s, d) \times \exp\left[N\mathbf{H}\left(\frac{s}{N}\right) + n \cdot \Psi(s, d, \epsilon)\right] \quad (105)$$

$$< k \left(\frac{5}{4}\right)^2 \frac{p_{max}(k, d)}{\sqrt{2\pi k(1 - \frac{k}{N})}} \times \exp\left[N\left(\mathbf{H}\left(\frac{k}{N}\right) + \frac{n}{N} \cdot \Psi(k, d, \epsilon)\right)\right]. \quad (106)$$

From (103) to (104) we bound the probability in (103) using Corollary 1.7. Then from (104) to (105) we bound $\binom{N}{s}$ using Stirling's formula (64) by a polynomial in N multiplying $p_{max}(s, d)$ and an exponential incorporated into the exponent of the exponential term. From (105) to (106) we use that for $N > 2k$ the entropy $\mathbf{H}\left(\frac{s}{N}\right)$ is largest when $s = k$ and 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 $p'_{max}(N, k, d) = k \left(\frac{5}{4}\right)^2 \frac{p_{max}(k, d)}{\sqrt{2\pi k(1 - \frac{k}{N})}}$ which simplifies to $\frac{1}{16\pi k \sqrt{d^3(1 - \frac{k}{N})}}$ and the factor $\Psi_{net}(k, n, N; d, \epsilon) = \mathbf{H}\left(\frac{k}{N}\right) + \frac{n}{N} \cdot \Psi(k, d, \epsilon)$ is what is multiplied to N in the exponent as claimed.

3) *Corollary 1.11*: Corollary 1.10 has given us an upper bound on the probability $\text{Prob}(\|Ax\|_1 \leq (1 - 2\epsilon)d\|x\|_1)$ in (9). In this bound the exponential dominates the polynomial. Consequently, in the limit as $(k, n, N) \rightarrow \infty$ while $k/n \rightarrow \rho \in (0, 1)$ and $n/N \rightarrow \delta \in (0, 1)$ this bound has a sharp transition at the zero level curve of Ψ_{net} . For $\Psi_{net}(k, n, N; d, \epsilon)$ strictly bounded above zero the overall bound grows exponentially in N without limit, while for $\Psi_{net}(k, n, N; d, \epsilon)$ strictly bounded below zero the overall bound decays to zero exponentially quickly. We define $\rho^{exp}(\delta; d, \epsilon)$ to satisfy $\Psi_{net}(k, n, N; d, \epsilon) = 0$ in (13), so that for any ρ strictly less than $\rho^{exp}(\delta; d, \epsilon)$ the exponent will satisfy $\Psi_{net}(k, n, N; d, \epsilon) < 0$ and hence the bound decay to zero.

More precisely, for $k/n \rightarrow \rho < (1 - \gamma)\rho^{exp}(\delta; d, \epsilon)$ with small $\gamma > 0$, in this regime of $\rho < (1 - \gamma)\rho^{exp}(\delta; d, \epsilon)$ we have $\text{Prob}(\|Ax\|_1 \leq (1 - 2\epsilon)d\|x\|_1) \rightarrow 0$. Therefore, $\text{Prob}(\|Ax\|_1 \geq (1 - 2\epsilon)d\|x\|_1) \rightarrow 1$ as the problem size grows such that $(k, n, N) \rightarrow \infty$, $n/N \rightarrow \delta \in (0, 1)$ and $k/n \rightarrow \rho$.

V. APPENDIX

A. Proof of Corollary 2.2

The first part of this proof uses ideas from the proof of Proposition 2.1 which is the same as Theorem 16 in [33]. 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 ϵds of these indices are in the collision set that is identical to some preceding value in the sequence.

Therefore, the probability that a neighbor chosen uniformly at random is to be in the collision set is at most ds/n and, treating each event independently, then the probability that a set of ϵds neighbors 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 ϵds 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

$$\begin{aligned} \text{Prob}(G \text{ fails to expand on } S) \\ \leq \binom{N}{s} \binom{ds}{\epsilon ds} \left(\frac{ds}{n}\right)^{\epsilon ds}. \end{aligned} \quad (107)$$

We define p_s to be the right hand side of (107) and we use the right hand side of the Stirling's inequality (64) to upper bound p_s as thus

$$\begin{aligned} p_s &< \frac{5}{4} \left[2\pi \frac{\epsilon ds}{ds} \left(1 - \frac{\epsilon ds}{ds}\right) \epsilon ds \right]^{-\frac{1}{2}} \exp \left[ds \text{H} \left(\frac{\epsilon ds}{ds} \right) \right] \\ &\quad \times \frac{5}{4} \left[2\pi \frac{s}{N} \left(1 - \frac{s}{N}\right) N \right]^{-\frac{1}{2}} \\ &\quad \times \exp \left[N \text{H} \left(\frac{s}{N} \right) \right] \times \left(\frac{ds}{n} \right)^{\epsilon ds} \end{aligned} \quad (108)$$

Writing the last multiplicand of (108) in exponential form and simplifying the expression gives

$$p_s < p_{max}(N, s; d, \epsilon) \cdot \exp[N \cdot \Psi(s, n, N; d, \epsilon)], \quad (109)$$

where $\Psi(s, n, N; d, \epsilon)$ is

$$\text{H} \left(\frac{s}{N} \right) + \frac{ds}{N} \text{H}(\epsilon) + \frac{\epsilon ds}{N} \log \left(\frac{ds}{n} \right), \quad (110)$$

and $p_{max}(N, s; d, \epsilon)$ is a polynomial in N and s for each d and ϵ fixed given by

$$\left(\frac{5}{4} \right)^2 \cdot \frac{1}{2\pi s} \cdot \left[\frac{N}{\epsilon(1 - \epsilon)(N - s)d} \right]^{\frac{1}{2}}. \quad (111)$$

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

$$\text{Prob}(G \text{ fails to be an expander}) \leq \sum_{s=1}^k p_s. \quad (112)$$

From (109) we have $\sum_{s=2}^k p_s$ bounded by

$$\sum_{s=2}^k p_{max}(N, s; d, \epsilon) \cdot \exp[N \cdot \Psi(s, n, N; d, \epsilon)] \quad (113)$$

$$< p'_{max}(N, k; d, \epsilon) \cdot \exp[N \cdot \Psi(k, n, N; d, \epsilon)], \quad (114)$$

where $p'_{max}(N, k; d, \epsilon) = k \cdot p_{max}(N, k; d, \epsilon)$ and we achieved the bound from (113) to (114) 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 (112) and (114) we have

$$\begin{aligned} \text{Prob}(G \text{ fails to be an expander}) &< p'_{max}(N, k; d, \epsilon) \\ &\quad \times \exp[N \cdot \Psi(k, n, N; d, \epsilon)]. \end{aligned} \quad (115)$$

As the problem size, (k, n, N) , grows the exponential term will be driving the probability in (115), hence having

$$\Psi(k, n, N; d, \epsilon) < 0 \quad (116)$$

yields $\text{Prob}(G \text{ fails to be an expander}) \rightarrow 0$ as the problem size $(k, n, N) \rightarrow \infty$.

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 $\rho_{bi}^{exp}(\delta; d, \epsilon)$ as the limiting value of k/n that satisfies $\Psi(k, n, N; d, \epsilon) = 0$ for each fixed ϵ and d and all δ . Note that for fixed ϵ , d and δ it is deducible from our analysis of $\psi_n(\cdot)$ in Section II-B that $\Psi(k, n, N; d, \epsilon)$ is a strictly monotonically increasing function of k/n . Therefore for any $\rho < \rho_{bi}^{exp}$, $\Psi(k, n, N; d, \epsilon) < 0$ as $(k, n, N) \rightarrow \infty$, $\text{Prob}(G \text{ fails to be an expander}) \rightarrow 0$ and G becomes an expander with probability approaching one exponentially in N which is the same as exponential growth in n since $n \rightarrow N\rho$.

REFERENCES

- [1] R. Horn and C. Johnson, *Matrix analysis*. Cambridge Univ Pr, 1990.
- [2] J. Demmel, *Numerical linear algebra*. Center for Pure and Applied Mathematics, Dept. of Mathematics, University of California, 1993, vol. 1.
- [3] L. Trefethen and D. Bau, *Numerical linear algebra*. Society for Industrial Mathematics, 1997, no. 50.
- [4] W. Xu and B. Hassibi, "Further results on performance analysis for compressive sensing using expander graphs," in *Signals, Systems and Computers, 2007. ACSSC 2007. Conference Record of the Forty-First Asilomar Conference on*. IEEE, 2007, pp. 621–625.
- [5] R. Berinde, A. Gilbert, P. Indyk, H. Karloff, and M. Strauss, "Combining geometry and combinatorics: A unified approach to sparse signal recovery," in *Communication, Control, and Computing, 2008 46th Annual Allerton Conference on*. IEEE, 2008, pp. 798–805.
- [6] R. Berinde and P. Indyk, "Sparse recovery using sparse random matrices," *preprint*, 2008.
- [7] S. Jafarpour, W. Xu, B. Hassibi, and R. Calderbank, "Efficient and robust compressed sensing using optimized expander graphs," *Information Theory, IEEE Transactions on*, vol. 55, no. 9, pp. 4299–4308, 2009.
- [8] J. Blanchard and J. Tanner, "Gpu accelerated greedy algorithms for compressed sensing," *Preprint*, 2012.
- [9] S. Hoory, N. Linial, and A. Wigderson, "Expander graphs and their applications," *Bulletin of the American Mathematical Society*, vol. 43, no. 4, pp. 439–562, 2006.
- [10] M. Capalbo, O. Reingold, S. Vadhan, and A. Wigderson, "Randomness conductors and constant-degree lossless expanders," in *Proceedings of the thirty-fourth annual ACM symposium on Theory of computing*. ACM, 2002, pp. 659–668.
- [11] L. Bassalygo and M. Pinsker, "Complexity of an optimum nonblocking switching network without reconstructions," *Problemy Peredachi Informatsii*, vol. 9, no. 1, pp. 84–87, 1973.
- [12] V. Guruswami, C. Umans, and S. Vadhan, "Unbalanced expanders and randomness extractors from parvaresh-vardy codes," 2007.
- [13] J. Blanchard, C. Cartis, J. Tanner, and A. Thompson, "Phase transitions for greedy sparse approximation algorithms," *Applied and Computational Harmonic Analysis*, vol. 30, no. 2, pp. 188–203, 2011.
- [14] R. G. Baranuik, "Compressive sensing," *IEEE Signal Processing Magazine*, vol. 118, 2007, lecture notes.
- [15] E. Candès and M. Wakin, "An introduction to compressive sampling," *Signal Processing Magazine, IEEE*, vol. 25, no. 2, pp. 21–30, 2008.
- [16] D. L. Donoho, "Compressed sensing," *IEEE Trans. Inform. Theory*, vol. 52, no. 4, pp. 1289–1306, 2006.
- [17] M. Lustig, D. Donoho, J. Santos, and J. Pauly, "Compressed sensing mri," *Signal Processing Magazine, IEEE*, vol. 25, no. 2, pp. 72–82, 2008.
- [18] T. Blumensath and M. E. Davies, "Iterative hard thresholding for compressed sensing," *Applied and Computational Harmonic Analysis*, April 2009.
- [19] E. J. Candès and T. Tao, "Decoding by linear programming," *IEEE Trans. Inform. Theory*, vol. 51, no. 12, pp. 4203–4215, 2005.
- [20] W. Dai and O. Milenkovic, "Subspace pursuit for compressive sensing signal reconstruction," *IEEE Trans. Inform. Theory*, vol. 55, no. 5, pp. 2230–2249, 2009.
- [21] S. Foucart and M.-J. Lai, "Sparsest solutions of underdetermined linear systems via ℓ_q -minimization for $0 < q \leq 1$," *Appl. Comput. Harmon. Anal.*, vol. 26, no. 3, pp. 395–407, 2009.
- [22] D. Needell and J. Tropp, "Cosamp: Iterative signal recovery from incomplete and inaccurate samples," *Appl. Comp. Harm. Anal.*, vol. 26, no. 3, pp. 301–321, 2009.
- [23] S. Jafarpour, W. Xu, B. Hassibi, and R. Calderbank, "Efficient and robust compressed sensing using high-quality expander graphs," *Arxiv preprint arXiv:0806.3802*, 2008.
- [24] W. Xu and B. Hassibi, "Efficient compressive sensing with deterministic guarantees using expander graphs," in *Information Theory Workshop, 2007. ITW'07. IEEE*. IEEE, 2007, pp. 414–419.
- [25] M. Pinsker, "On the complexity of a concentrator," in *7th annual teletraffic conference*, 1973, p. 318.
- [26] T. Blumensath and M. E. Davies, "Normalized iterative hard thresholding: guaranteed stability and performance," *IEEE Journal of Selected Topics in Signal Processing*, vol. 4(2), pp. 298–309, 2010.
- [27] P. Indyk and M. Ruzic, "Near-optimal sparse recovery in the ℓ_1 norm," in *Foundations of Computer Science, 2008. FOCS'08. IEEE 49th Annual IEEE Symposium on*. IEEE, 2008, pp. 199–207.
- [28] R. Berinde, P. Indyk, and M. Ruzic, "Practical near-optimal sparse recovery in the ℓ_1 norm," in *Communication, Control, and Computing, 2008 46th Annual Allerton Conference on*. IEEE, 2008, pp. 198–205.
- [29] R. Berinde and P. Indyk, "Sequential sparse matching pursuit," in *Communication, Control, and Computing, 2009. Allerton 2009. 47th Annual Allerton Conference on*. IEEE, 2009, pp. 36–43.
- [30] E. J. Candès, "The restricted isometry property and its implications for compressed sensing," *C. R. Math. Acad. Sci. Paris*, vol. 346, no. 9–10, pp. 589–592, 2008.
- [31] J. Blanchard, C. Cartis, and J. Tanner, "Compressed sensing: How sharp is the restricted isometry property?" *SIAM Review*, vol. 53, no. 1, pp. 105–125, 2011.
- [32] B. Bah and J. Tanner, "Improved bounds on restricted isometry constants for gaussian matrices," *SIAM Journal of Matrix Analysis*, 2010.
- [33] R. Berinde, "Advances in sparse signal recovery methods," Master's thesis, Massachusetts Institute of Technology, 2009.

Bubacarr Bah Bubacarr Bah received the BSc degree in mathematics and physics from the University of The Gambia, and the MSc degree in mathematical modeling and scientific computing from the University of Oxford, Wolfson College. He is currently a postgraduate student in applied and computational mathematics at the University of Edinburgh where his PhD supervisor is Jared Tanner. Previously he had been a Graduate Assistant at the University of The Gambia (2004–2007). His research interests include random matrix theory with applications to compressed sensing and sparse approximation. Bubacarr has received the SIAM Best Student Paper Prize (2010).

Jared Tanner Jared Tanner received the B.S. degree in physics from the University of Utah, and the Ph.D. degree in Applied Mathematics from UCLA where his PhD adviser was Eitan Tadmor. He is currently the Professor of the mathematics of information at the University of Oxford and Fellow of Exeter College. Previously he had the academic posts: Professor of the mathematics of information at the University of Edinburgh (2007–2012), Assistant Professor at the University of Utah (2006–2007), National Science Foundation postdoctoral fellow in the mathematical sciences at Stanford University (2004–2006), and a Visiting Assistant Research Professor at the University of California at Davis (2002–2004). His research interests include signal processing with emphasis in compressed sensing, sparse approximation, applied Fourier analysis, and spectral methods. Professor Tanner has received the Philip Leverhulme Prize (2009), Sloan Research Fellow in Science and Technology (2007), Monroe Martin Prize (2005), and the Leslie Fox Prize (2003).