

A Simple Proof that Random Matrices are Democratic

Mark A. Davenport, Jason N. Laska, Petros T. Boufounos,
and Richard G. Baraniuk*

Rice University
Department of Electrical and Computer Engineering
Technical Report TREE0906

November 4, 2009

Abstract

The recently introduced theory of *compressive sensing* (CS) enables the reconstruction of sparse or compressible signals from a small set of nonadaptive, linear measurements. If properly chosen, the number of measurements can be significantly smaller than the ambient dimension of the signal and yet preserve the significant signal information. Interestingly, it can be shown that random measurement schemes provide a near-optimal encoding in terms of the required number of measurements. In this report, we explore another relatively unexplored, though often alluded to, advantage of using random matrices to acquire CS measurements. Specifically, we show that random matrices are *democratic*, meaning that each measurement carries roughly the same amount of signal information. We demonstrate that by slightly increasing the number of measurements, the system is robust to the loss of a small number of arbitrary measurements. In addition, we draw connections to oversampling and demonstrate stability from the loss of significantly more measurements.

1 Introduction

The recently developed *compressive sensing* (CS) framework allows us to acquire a signal $\mathbf{x} \in \mathbb{R}^N$ from a small set of M non-adaptive, linear measurements [1, 2]. This process can be represented as

$$\mathbf{y} = \Phi \mathbf{x} \quad (1)$$

where Φ is an $M \times N$ matrix that models the measurement system. The hope is that we can design Φ so that \mathbf{x} can be accurately recovered even when $M \ll N$. In general this is not possible, but if \mathbf{x} is K -sparse, meaning that it has only K nonzero entries then it is possible to design Φ that preserve the information about \mathbf{x} using only $M = O(K \log(N/K))$ measurements. The most commonly studied Φ that satisfy this bound on M are *random*, i.e., each entry of Φ is drawn independently from some suitable distribution [3]. We will focus our attention on such Φ .

*MAD, JNL, and RGB are with the Department of Electrical and Computer Engineering, Rice University, Houston, TX, USA. Email: {md, laska, richb}@rice.edu.

PTB is with Mitsubishi Electric Research Laboratories (MERL), Boston, MA, USA. Email: petrosb@merl.com.

This work was supported by the grants NSF CCF-0431150, CCF-0728867, CNS-0435425, and CNS-0520280, DARPA/ONR N66001-08-1-2065, ONR N00014-07-1-0936, N00014-08-1-1067, N00014-08-1-1112, and N00014-08-1-1066, AFOSR FA9550-07-1-0301, ARO MURI W311NF-07-1-0185, and the Texas Instruments Leadership University Program.

Web: dsp.rice.edu/cs

Among the advantages of random measurements is a property commonly referred to as *democracy*. While it is not usually rigorously defined in the literature, democracy is usually taken to mean that each measurement contributes a similar amount of information about the signal \mathbf{x} to the compressed representation \mathbf{y} [4–6].¹ Others have described democracy to mean that each measurement is equally important (or unimportant) [7]. Despite the fact that democracy is so frequently touted as an advantage of random measurements, it has received little analytical attention in the CS context. Perhaps more surprisingly, the property has not been explicitly exploited in applications until recently [8].

The fact that random measurements are democratic seems intuitive; when using random measurements, each measurement is a randomly weighted sum of a large fraction (or all) of the entries of \mathbf{x} , and since the weights are chosen independently at random, no preference is given to any particular entries. More concretely, suppose that the measurements y_1, y_2, \dots, y_M are independent and identically distributed (i.i.d.) according to some distribution f_Y , as is the case for the Φ considered in this report. Now suppose that we select $\widetilde{M} < M$ of the y_i at random (or according to some procedure that is *independent* of \mathbf{y}). Then clearly, we are left with a length- \widetilde{M} measurement vector $\widetilde{\mathbf{y}}$ such that each $\widetilde{y}_i \sim f_Y$. Stated another way, if we set $D = M - \widetilde{M}$, then there is no difference between collecting \widetilde{M} measurements and collecting M measurements and deleting D of them, provided that this deletion is done independently of the actual values of \mathbf{y} .

However, following this line of reasoning will ultimately lead to a rather weak definition of democracy. To see this, consider the case where the measurements are deleted by an adversary. By adaptively deleting the entries of \mathbf{y} one can change the distribution of $\widetilde{\mathbf{y}}$. For example, the adversary can delete the D largest elements of \mathbf{y} , thereby skewing the distribution of $\widetilde{\mathbf{y}}$. In many cases, especially if the same matrix Φ will be used repeatedly with different measurements being deleted each time, it would be far better to know that *any* \widetilde{M} measurements will be sufficient to reconstruct the signal. This is a significantly stronger requirement.

In order to formally define this stronger notion of democracy, we must first describe the properties that a matrix must satisfy to ensure stable reconstruction. Towards that end, we recall the definition of the *restricted isometry property* (RIP) for the matrix Φ [9].

Definition 1. A matrix Φ satisfies the RIP of order K with constant $\delta \in (0, 1)$ if

$$(1 - \delta)\|\mathbf{x}\|_2^2 \leq \|\Phi\mathbf{x}\|_2^2 \leq (1 + \delta)\|\mathbf{x}\|_2^2 \quad (2)$$

holds for all \mathbf{x} such that $\|\mathbf{x}\|_0 \leq K$.

Much is known about matrices that satisfy the RIP, but for our purposes it suffices to note that if we draw a random $M \times N$ matrix Φ whose entries ϕ_{ij} are i.i.d. sub-Gaussian random variables, then provided that

$$M = O(K \log(N/K)), \quad (3)$$

we have that with high probability Φ will satisfy the RIP of order K with constant δ [3, 10].

When it is satisfied, the RIP for a matrix Φ provides a sufficient condition to guarantee successful sparse recovery using a wide variety of algorithms [9, 11–20]. As an example, the RIP of order $2K$ (with isometry constant $\delta < \sqrt{2} - 1$) is a sufficient condition to permit ℓ_1 -minimization (the canonical convex optimization problem for sparse approximation) to exactly recover any K -sparse signal and to approximately recover those that are nearly sparse [11]. The same assumption is also a sufficient condition for robust recovery in noise using a modified ℓ_1 -minimization [11].

¹The original introduction of this term was with respect to quantization [4, 5], i.e., a democratic quantizer would ensure that each bit is given “equal weight.” As the CS framework developed, it became empirically clear that CS systems exhibited this property with respect to compression [6].

The RIP also provides us with a way to quantify our notion of democracy. To do so, we first establish some notation that will prove useful throughout this report. Let $\Gamma \subset \{1, 2, \dots, M\}$. By Φ^Γ we mean the $|\Gamma| \times M$ matrix obtained by selecting the rows of Φ indexed by Γ . Alternatively, if $\Lambda \subset \{1, 2, \dots, N\}$, then we use Φ_Λ to indicate the $M \times |\Lambda|$ matrix obtained by selecting the columns of Φ indexed by Λ . Following [8], we now formally define democracy as follows.

Definition 2. Let Φ be an $M \times N$ matrix, and let $\widetilde{M} \leq M$ be given. We say that Φ is $(\widetilde{M}, K, \delta)$ -democratic if for all Γ such that $|\Gamma| \geq \widetilde{M}$ the matrix Φ^Γ satisfies the RIP of order K with constant δ .

In Section 2 below we present a simple proof that Gaussian matrices are democratic and demonstrate how the proof can be extended to sub-Gaussian matrices. The core of this proof can be found in [8], but is included in full in this report. In Section 3 we discuss the implications of the result and alternative interpretations. Section 4 contains the additional theorems required by the proof.

2 Random matrices are democratic

We now demonstrate that certain randomly generated matrices are democratic. While the theorem actually holds (with different constants) for the more general class of *sub-Gaussian* matrices, for simplicity we restrict our attention to Gaussian matrices. We provide discussion of the sub-Gaussian case in Section 4.

Theorem 1. Let Φ be an $M \times N$ matrix with elements ϕ_{ij} drawn according to $\mathcal{N}(0, 1/M)$ and let $\widetilde{M} \leq M$, $K < \widetilde{M}$, and $\delta \in (0, 1)$ be given. Define $D = M - \widetilde{M}$. If

$$M = C_1(K + D) \log \left(\frac{N + M}{K + D} \right), \quad (4)$$

then with probability exceeding $1 - 3e^{-C_2 M}$ we have that Φ is $(\widetilde{M}, K, \delta/(1 - \delta))$ -democratic, where C_1 is arbitrary and $C_2 = (\delta/8)^2 - \log(42e/\delta)/C_1$.

Proof. Our proof consists of two main steps. We begin by defining the $M \times (N + M)$ matrix $\mathbf{A} = [\mathbf{I} \ \Phi]$ formed by appending Φ to the $M \times M$ identity matrix. Theorem 2, also found in [21], demonstrates that under the assumptions in the theorem statement, with probability exceeding $1 - 3e^{-C_2 M}$ we have that \mathbf{A} satisfies the RIP of order $K + D$ with constant δ . The second step is to use this fact to show that all possible $\widetilde{M} \times N$ submatrices of Φ satisfy the RIP of order K with constant $\delta/(1 - \delta)$.

Towards this end, we let $\Gamma \subset \{1, 2, \dots, M\}$ be an arbitrary subset of rows such that $|\Gamma| \geq \widetilde{M}$. Define $\Lambda = \{1, 2, \dots, N\} \setminus \Gamma$ and note that $|\Lambda| = D$. Additionally, let

$$\mathbf{P}_\Lambda \triangleq \mathbf{A}_\Lambda \mathbf{A}_\Lambda^\dagger, \quad (5)$$

be the orthogonal projector onto $\mathcal{R}(\mathbf{A}_\Lambda)$, i.e., the range, or column space, of \mathbf{A}_Λ .² Furthermore, we define

$$\mathbf{P}_\Lambda^\perp \triangleq \mathbf{I} - \mathbf{P}_\Lambda, \quad (6)$$

as the orthogonal projector onto the orthogonal complement of $\mathcal{R}(\mathbf{A}_\Lambda)$. In words, this projector nulls the columns of \mathbf{A} corresponding to the index set Λ . Now, note that $\Lambda \subset \{1, 2, \dots, N\}$, so $\mathbf{A}_\Lambda = \mathbf{I}_\Lambda$. Thus,

$$\mathbf{P}_\Lambda = \mathbf{I}_\Lambda \mathbf{I}_\Lambda^\dagger = \mathbf{I}_\Lambda (\mathbf{I}_\Lambda^T \mathbf{I}_\Lambda)^{-1} \mathbf{I}_\Lambda^T = \mathbf{I}_\Lambda \mathbf{I}_\Lambda^T = \mathbf{I}(\Lambda),$$

² $\mathbf{A}_\Lambda^\dagger = (\mathbf{A}_\Lambda^T \mathbf{A}_\Lambda)^{-1} \mathbf{A}_\Lambda^T$ denotes the Moore-Penrose pseudoinverse of \mathbf{A}_Λ .

where we use $\mathbf{I}(\Lambda)$ to denote the $M \times M$ matrix with all zeros except for ones on the diagonal entries corresponding to the columns indexed by Λ . (We distinguish the $M \times M$ matrix $\mathbf{I}(\Lambda)$ from the $M \times D$ matrix \mathbf{I}_Λ — in the former case we replace columns not indexed by Λ with zero columns, while in the latter we remove these columns to form a smaller matrix.) Similarly, we have

$$\mathbf{P}_\Lambda^\perp = \mathbf{I} - \mathbf{P}_\Lambda = \mathbf{I}(\Gamma).$$

Thus, we observe that the matrix $\mathbf{P}_\Lambda^\perp \mathbf{A} = \mathbf{I}(\Gamma) \mathbf{A}$ is simply the matrix \mathbf{A} with zeros replacing all entries on any row i such that $i \notin \Gamma$, i.e., $(\mathbf{P}_\Lambda^\perp \mathbf{A})^\Gamma = \mathbf{A}^\Gamma$ and $(\mathbf{P}_\Lambda^\perp \mathbf{A})^\Lambda = \mathbf{0}$. Furthermore, Theorem 3, also found in [22], states that for \mathbf{A} satisfying the RIP of order $K + D$ with constant δ , we have that

$$\left(1 - \frac{\delta}{1 - \delta}\right) \|\mathbf{u}\|_2^2 \leq \|\mathbf{P}_\Lambda^\perp \mathbf{A} \mathbf{u}\|_2^2 \leq (1 + \delta) \|\mathbf{u}\|_2^2, \quad (7)$$

holds for all $\mathbf{u} \in \mathbb{R}^{N+M}$ such that $\|\mathbf{u}\|_0 = K + D - |\Lambda| = K$ and $\text{supp}(\mathbf{u}) \cap \Lambda = \emptyset$. Equivalently, letting $\Lambda^c = \{1, 2, \dots, N + M\} \setminus \Lambda$, this result states that $(\mathbf{I}(\Gamma) \mathbf{A})_{\Lambda^c}$ satisfies the RIP of order K with constant $\delta/(1 - \delta)$. To complete the proof, we note that if $(\mathbf{I}(\Gamma) \mathbf{A})_{\Lambda^c}$ satisfies the RIP of order K with constant $\delta/(1 - \delta)$, then we trivially have that $\mathbf{I}(\Gamma) \Phi$ also has the RIP of order at least K with constant $\delta/(1 - \delta)$, since $\mathbf{I}(\Gamma) \Phi$ is just a submatrix of $(\mathbf{I}(\Gamma) \mathbf{A})_{\Lambda^c}$. Since $\|\mathbf{I}(\Gamma) \Phi \mathbf{x}\|_2 = \|\Phi^\Gamma \mathbf{x}\|_2$, this establishes the theorem. \square

3 Discussion

3.1 Robustness and stability

Observe that we require roughly $O(D \log(N))$ additional measurements to ensure that Φ is $(\widetilde{M}, K, \delta)$ -democratic compared to the number of measurements required to simply ensure that Φ satisfies the RIP of order K . This seems intuitive; if we wish to be robust to the loss of any D measurements while retaining the RIP of order K , then we should expect to take *at least* D additional measurements. This is not unique to the CS framework. For instance, by *oversampling*, i.e., sampling faster than the minimum required Nyquist rate, uniform sampling systems can also improve robustness with respect to the loss of measurements. However, a benefit of the democratic CS system is that the number of additional measurements needed grows more slowly than in the Nyquist case. To see this, consider the case where we lose D samples or measurements. For a fixed time period, suppose that sampling the signal at the Nyquist rate yields N samples. To be robust to the loss of a contiguous block of D samples, we must sample at $D + 1$ times the Nyquist rate, yielding DN additional samples. In contrast, the number of additional measurements needed for a CS measurement system to be democratic is $O(D \log(N))$, given by (4). Thus, the number of additional samples required by a Nyquist sampler depends linearly on D and N while the number of additional measurements for democratic CS systems is still linear in D but only *logarithmic* in N . If N is large, this can result in tremendous savings. Note also that for a fixed N and K , by driving M higher a CS measurement system can be robust to the loss of a large fraction of the acquired measurements, whereas in Nyquist oversampling, the fraction of (consecutive) samples that can be dropped can never exceed $1/N$.

In some applications, this difference may have significant impact. For example, in finite dynamic range quantizers, the measurements saturate when their magnitude exceeds some level. Thus, when uniformly sampling with a low saturation level, if one sample saturates, then the likelihood that any of the neighboring samples will saturate is high, and significant oversampling may be required

to ensure any benefit. However, in CS, if many adjacent measurements were to saturate, then for only a slight increase in the number of measurements we can mitigate this kind of error by simply rejecting the saturated measurements; the fact that Φ is democratic ensures that this strategy will be effective.

In addition to robustness, Theorem 1 implies that reconstruction from a subset of CS measurements is *stable* to the loss of a potentially larger number of measurements than anticipated. To see this, suppose that an $M \times N$ matrix Φ is $(M - D, K, \delta)$ -democratic, but consider the situation where $D + \tilde{D}$ measurements are dropped. It is clear from the proof of Theorem 1 that if $\tilde{D} < K$, then the resulting matrix Φ^Γ will satisfy the RIP of order $K - \tilde{D}$ with constant δ . Thus, from [23], if we define $\tilde{K} = (K - \tilde{D})/2$, then the reconstruction error is then bounded by

$$\|\mathbf{x} - \hat{\mathbf{x}}\|_2 \leq C_3 \frac{\|\mathbf{x} - \mathbf{x}_{\tilde{K}}\|_1}{\sqrt{\tilde{K}}}, \quad (8)$$

where $\mathbf{x}_{\tilde{K}}$ denotes the best \tilde{K} -term approximation of \mathbf{x} and C_3 is an absolute constant depending on Φ that can be bounded using the constants derived in Theorem 1. Thus, if \tilde{D} is small then the additional error caused by dropping too many measurements will also be relatively small. In contrast, there is simply no analog to this kind of stability result for uniform sampling with linear reconstruction. When the number of dropped samples exceeds D (where D represents the oversampling factor described above), there are no guarantees as to the accuracy of the reconstruction.

3.2 Numerical exploration

As discussed previously, the democracy property is a stronger condition than the RIP. To demonstrate this, we perform a numerical simulation which illustrates this point. Specifically, we would like to compare the case where the measurements are dropped at random versus the case where the dropped measurements are selected by an adversary. Ideally, we would like to know whether the resulting matrices satisfy the RIP. Of course, this experiment is impossible to perform for two reasons: first, determining if a matrix satisfies the RIP is computationally intractable as it would require checking all possible K -dimensional sub-matrices of Φ^Γ . Moreover, in the adversarial setting one would also have to search for the worst possible Γ as well, which is impossible for the same reason. Thus, we instead perform a far simpler experiment, which serves as a very rough proxy to the experiment we would like to perform.

The experiment proceeds over 100 trials as follows. We fix the parameters $N = 2048$ and $K = 13$ and vary M in the range $(0, 380)$. In each trial we draw a new matrix Φ with $\phi_{ij} \sim \mathcal{N}(0, 1/M)$ and a new signal with K nonzero coefficients, also drawn from a Gaussian distribution, and then the signal is normalized $\|\mathbf{x}\|_2 = 1$. Over each set of trials we estimate two quantities:

1. the maximum D such that we achieve exact reconstruction for a randomly selected $(M - D) \times N$ submatrix of Φ on each of the 100 trials;
2. the maximum D such that we achieve exact reconstruction for $R = 300$ randomly selected $(M - D) \times N$ submatrices of Φ on each of the 100 trials..

Ideally, the second case should consider *all* $(M - D) \times N$ submatrices of Φ rather than just 300 submatrices, but as this is not possible (for reasons discussed above) we simply perform a random sampling of the space of possible submatrices. Note also that exact recovery on one signal is also *not* proof that the matrix satisfies the RIP, although failure *is* proof that the matrix does not.

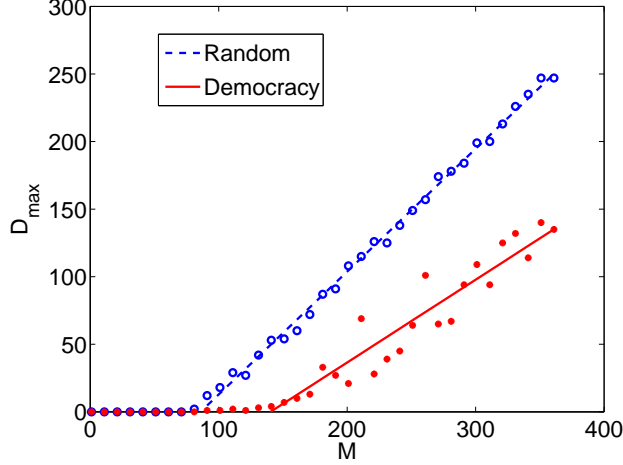


Figure 1: Maximum number of measurements that can be dropped D_{\max} vs. number of measurements M for (a) exact recovery of one $(M - D) \times N$ submatrix of Φ and (b) exact recovery of $R = 300$ $(M - D) \times N$ submatrices of Φ .

The results of this experiment are depicted in Figure 1. The circles denote data points with the empty circles corresponding to the random selection experiment and the solid circles corresponding to the democracy experiment. The lines denote the best linear fit for each data set where $D > 0$, with the dashed line corresponding to the random selection experiment and the solid line corresponding to democracy experiment.

The maximum D corresponding to the random selection experiment grows linearly in M (with coefficient 1) once the minimum number of measurements required for RIP, denoted by M' , is reached. This is because beyond this point at most $D = M - M'$ measurements can be discarded. As demonstrated by the plot, $M' \approx 90$ for this experiment. For the democracy experiment $M' \approx 150$, larger than for the RIP experiment. Furthermore, the maximum D for democracy grows more slowly than for the random selection case, which indicates that to be robust to the loss of *any* D measurements, CD additional measurements, with $C > 1$, are actually *necessary*.

4 Theorems

In this section, we prove the two supporting Theorems used in the proof of Theorem 1. We begin by demonstrating that the matrix $\mathbf{A} = [\mathbf{I} \ \Phi]$ satisfies the RIP. To do so, we first establish the following lemma, that closely parallels the result in equation (4.3) of [3]. The lemma demonstrates that for any \mathbf{u} , if we draw Φ at random, then $\|\mathbf{A}\mathbf{u}\|_2$ is concentrated around $\|\mathbf{u}\|_2$.

Lemma 1. *Let Φ be an $M \times N$ matrix with elements ϕ_{ij} drawn i.i.d. according to $\mathcal{N}(0, 1/M)$ and let $\mathbf{A} = [\mathbf{I} \ \Phi]$. Furthermore, let $\mathbf{u} \in \mathbb{R}^{N+M}$ be an arbitrary vector with first M entries denoted by \mathbf{w} and last N entries denoted by \mathbf{x} . Let $\eta \in (0, 1)$ be given. Then*

$$\mathbb{E} (\|\mathbf{A}\mathbf{u}\|_2^2) = \|\mathbf{u}\|_2^2 \quad (9)$$

and

$$\mathbb{P} (|\|\mathbf{A}\mathbf{u}\|_2^2 - \|\mathbf{u}\|_2^2| \geq 2\eta\|\mathbf{u}\|_2^2) \leq 3e^{-M\eta^2/8}. \quad (10)$$

Proof. We first note that since $\mathbf{A}\mathbf{u} = \mathbf{w} + \Phi\mathbf{x}$, we have that

$$\begin{aligned}
\|\mathbf{A}\mathbf{u}\|_2^2 &= \|\mathbf{w} + \Phi\mathbf{x}\|_2^2 \\
&= (\mathbf{w} + \Phi\mathbf{x})^T (\mathbf{w} + \Phi\mathbf{x}) \\
&= \mathbf{w}^T \mathbf{w} + 2\mathbf{w}^T \Phi\mathbf{x} + \mathbf{x}^T \Phi^T \Phi\mathbf{x} \\
&= \|\mathbf{w}\|_2^2 + 2\mathbf{w}^T \Phi\mathbf{x} + \|\Phi\mathbf{x}\|_2^2.
\end{aligned} \tag{11}$$

Since the entries ϕ_{ij} are i.i.d. according to $\mathcal{N}(0, 1/M)$, it is straightforward to show that $\mathbb{E}(\|\Phi\mathbf{x}\|_2^2) = \|\mathbf{x}\|_2^2$ (see, for example, [24]). Similarly, one can also show that $2\mathbf{w}^T \Phi\mathbf{x} \sim \mathcal{N}(0, 4\|\mathbf{w}\|_2^2 \|\mathbf{x}\|_2^2 / M)$, since the elements of $\Phi\mathbf{x}$ are distributed as zero mean Gaussian variables with variance $\|\mathbf{x}\|_2^2 / M$. Thus, from (11) we have that

$$\mathbb{E}(\|\mathbf{A}\mathbf{u}\|_2^2) = \|\mathbf{w}\|_2^2 + \|\mathbf{x}\|_2^2,$$

and since $\|\mathbf{u}\|_2^2 = \|\mathbf{w}\|_2^2 + \|\mathbf{x}\|_2^2$, this establishes (9).

We now turn to (10). Using the arguments in [24], one can show that

$$\mathbb{P}(|\|\Phi\mathbf{x}\|_2^2 - \|\mathbf{x}\|_2^2| \geq \eta\|\mathbf{x}\|_2^2) \leq 2e^{-M\eta^2/8}. \tag{12}$$

As noted above, $2\mathbf{w}^T \Phi\mathbf{x} \sim \mathcal{N}(0, 4\|\mathbf{w}\|_2^2 \|\mathbf{x}\|_2^2 / M)$. Hence, we have that

$$\begin{aligned}
\mathbb{P}(|2\mathbf{w}^T \Phi\mathbf{x}| \geq \eta\|\mathbf{w}\|_2 \|\mathbf{x}\|_2) &= 2Q\left(\frac{\eta\|\mathbf{w}\|_2 \|\mathbf{x}\|_2}{2\|\mathbf{w}\|_2 \|\mathbf{x}\|_2 / \sqrt{M}}\right) \\
&= 2Q(\sqrt{M}\eta/2),
\end{aligned}$$

where $Q(\cdot)$ denotes the tail integral of the standard Gaussian distribution. From (13.48) of [25] we have that

$$Q(z) \leq \frac{1}{2}e^{-z^2/2}$$

and thus we obtain

$$\mathbb{P}(|2\mathbf{w}^T \Phi\mathbf{x}| \geq \eta\|\mathbf{w}\|_2 \|\mathbf{x}\|_2) \leq e^{-M\eta^2/8}. \tag{13}$$

Thus, combining (12) and (13) we obtain that with probability at least $1 - 3e^{-M\eta^2/8}$ we have that both

$$(1 - \eta)\|\mathbf{x}\|_2^2 \leq \|\Phi\mathbf{x}\|_2^2 \leq (1 + \eta)\|\mathbf{x}\|_2^2 \tag{14}$$

and

$$-\eta\|\mathbf{w}\|_2 \|\mathbf{x}\|_2 \leq 2\mathbf{w}^T \Phi\mathbf{x} \leq \eta\|\mathbf{w}\|_2 \|\mathbf{x}\|_2. \tag{15}$$

Using (11), we can combine (14) and (15) to obtain

$$\begin{aligned}
\|\mathbf{A}\mathbf{u}\|_2^2 &\leq \|\mathbf{w}\|_2^2 + \eta\|\mathbf{w}\|_2 \|\mathbf{x}\|_2 + (1 + \eta)\|\mathbf{x}\|_2^2 \\
&\leq (1 + \eta)(\|\mathbf{w}\|_2^2 + \|\mathbf{x}\|_2^2) + \eta\|\mathbf{w}\|_2 \|\mathbf{x}\|_2 \\
&\leq (1 + \eta)\|\mathbf{u}\|_2^2 + \eta\|\mathbf{u}\|_2^2 \\
&= (1 + 2\eta)\|\mathbf{u}\|_2^2,
\end{aligned}$$

where the last inequality follows from the fact that $\|\mathbf{w}\|_2 \|\mathbf{x}\|_2 \leq \|\mathbf{u}\|_2 \|\mathbf{u}\|_2$. Similarly, we also have that

$$\|\mathbf{A}\mathbf{u}\|_2^2 \geq (1 - 2\eta)\|\mathbf{u}\|_2^2,$$

which establishes (10). \square

We note that while the above proof assumes that the entries of Φ are Gaussian, this proof holds with essentially no modifications for a wide class of *sub-Gaussian* distributions. A random variable X is sub-Gaussian if there exists a constant $C > 0$ such that

$$\mathbb{E}(e^{Xt}) \leq e^{C^2 t^2 / 2} \quad (16)$$

for all $t \in \mathbb{R}$. This says that the moment-generating function of our distribution is dominated by that of a Gaussian distribution, which is also equivalent to requiring that the tails of our distribution decay *at least as fast* as the tails of a Gaussian distribution. Examples of sub-Gaussian distributions include the Gaussian distribution, the Rademacher distribution, and the uniform distribution. In general, any distribution with bounded support is sub-Gaussian. See [26] for more discussion on sub-Gaussian random variables. It can be shown (see Lemma 6.1 of [10] or [27]) that if the entries of Φ are drawn according to a sub-Gaussian distribution, then (12) holds where 8 is replaced with a constant that depends on the constant C in (16). Similarly, the cross-term $|2\mathbf{w}^T \Phi \mathbf{x}|$ is also a sub-Gaussian random variable, and so using elementary results in [26], a bound analogous to (13) can be obtained.

Using Lemma 1, we now demonstrate that the matrix \mathbf{A} satisfies the RIP provided that M is sufficiently large.

Theorem 2. *Let Φ be an $M \times N$ matrix with elements ϕ_{ij} drawn according to $\mathcal{N}(0, 1/M)$ and let $\mathbf{A} = [\mathbf{I} \ \Phi]$. If*

$$M = C_1(K + D) \log \left(\frac{N + M}{K + D} \right) \quad (17)$$

then with probability exceeding $1 - 3e^{-C_2 M}$ we have that \mathbf{A} satisfies the RIP of order $(K + D)$ with constant δ , where C_1 is arbitrary and $C_2 = (\delta/8)^2 - \log(42e/\delta)/C_1$.

Proof. First note that it is enough to prove (17) in the case $\|\mathbf{x}\|_2 = 1$, since \mathbf{A} is linear. Next, fix an index set $J \subset \{1, 2, \dots, N + M\}$ with $|J| = K + D$, and let X_J denote the $(K + D)$ -dimensional subspace spanned by the columns of \mathbf{A} indexed by J . We choose a finite set of points S_J such that $S_J \subseteq X_J$, $\|\mathbf{s}\|_2 \leq 1$ for all $\mathbf{s} \in S_J$, and for all $\mathbf{x} \in X_J$ with $\|\mathbf{x}\|_2 \leq 1$ we have

$$\min_{\mathbf{s} \in S_J} \|\mathbf{x} - \mathbf{s}\|_2 \leq \epsilon. \quad (18)$$

One can show (see Chapter 15 of [28]) that such a set S_J exists with $|S_J| \leq (3/\epsilon)^{K+D}$. We then repeat this process for each possible index set J , and collect all the sets S_J together

$$S = \bigcup_{J: |J|=K+D} S_J. \quad (19)$$

There are $\binom{N+M}{K+D} \leq \left(e \frac{N+M}{K+D}\right)^{K+D}$ possible index sets J , and hence $|S| \leq \left(\frac{3e}{\epsilon} \frac{N+M}{K+D}\right)^{K+D}$. We now use the union bound to apply Lemma 1 to this set of points such that, with probability exceeding

$$1 - 3 \left(\frac{3e}{\epsilon} \frac{N+M}{K+D} \right)^{K+D} e^{-\frac{M\eta^2}{8}} = 1 - 3e^{-\frac{M\eta^2}{8} + (K+D) \log\left(\frac{3e}{\epsilon} \frac{N+M}{K+D}\right)}, \quad (20)$$

we have

$$(1 - 2\eta)\|\mathbf{s}\|_2^2 \leq \|\mathbf{A}\mathbf{s}\|_2^2 \leq (1 + 2\eta)\|\mathbf{s}\|_2^2, \quad \text{for all } \mathbf{s} \in S.$$

We now define $\Sigma_{K+D} = \{\mathbf{x} : \|\mathbf{x}\|_0 \leq K + D\}$. We define B as the smallest number such that

$$\|\mathbf{A}\mathbf{x}\|_2^2 \leq B\|\mathbf{x}\|_2^2, \quad \text{for all } \mathbf{x} \in \Sigma_{K+D}, \|\mathbf{x}\|_2 \leq 1. \quad (21)$$

Our goal is to show that $B \leq \sqrt{1+\delta}$. For this, we recall that for any $\mathbf{x} \in \Sigma_{K+D}$ with $\|\mathbf{x}\|_2 \leq 1$, we can pick a $\mathbf{s} \in S$ such that $\|\mathbf{x} - \mathbf{s}\|_2 \leq \epsilon$ and such that $\mathbf{x} - \mathbf{s} \in \Sigma_{K+D}$ (since if $\mathbf{x} \in X_J$, we can pick $\mathbf{s} \in S_J \subset X_J$ satisfying $\|\mathbf{x} - \mathbf{s}\|_2 \leq \epsilon$). In this case we have

$$\|\mathbf{A}\mathbf{x}\|_2 \leq \|\mathbf{A}\mathbf{s}\|_2 + \|\mathbf{A}(\mathbf{x} - \mathbf{s})\|_2 \leq \sqrt{1+2\eta} + \sqrt{B}\epsilon.$$

Since by definition B is the smallest number for which (21) holds, we obtain $\sqrt{B} \leq \sqrt{1+2\eta} + \sqrt{B}\epsilon$, which upon rearranging yields $\sqrt{B} \leq \sqrt{1+2\eta}/(1-\epsilon)$. One can show that by setting $\epsilon = \delta/14$ and $\eta = \delta/2\sqrt{2}$, we have that $\sqrt{1+2\eta}/(1-\epsilon) \leq \sqrt{1+\delta}$, which establishes the upper inequality in (2). The lower inequality follows from this since

$$\|\mathbf{A}\mathbf{x}\|_2 \geq \|\mathbf{A}\mathbf{s}\|_2 - \|\mathbf{A}(\mathbf{x} - \mathbf{s})\|_2 \geq \sqrt{1-2\eta} - \sqrt{1+\delta} \frac{\epsilon}{1-\epsilon} \geq \sqrt{1-\delta},$$

where the last inequality again holds with $\epsilon = \delta/14$ and $\eta = \delta/2\sqrt{2}$. This establishes the theorem. To arrive at the formula for C_2 we first bound the result in (20) using

$$\log \left(\frac{3e}{\epsilon} \frac{N+M}{K+D} \right) \leq \log \left(\frac{3e}{\epsilon} \right) \log \left(\frac{N+M}{K+D} \right)$$

and then we replace $(K+D) \log((N+M)/(K+D))$ with M/C_1 . After simplification, this yields $C_2 = \eta^2/8 - \log(3e/\epsilon)/C_1$. By substituting the values for ϵ and η , we obtain the desired result. \square

In Theorem 3 below, we show that the matrix $\mathbf{P}_\Lambda^\perp \mathbf{A}$ satisfies a modified version of the RIP. We begin with an elementary lemma that is a straightforward generalization of Lemma 2.1 of [11], and states that RIP operators approximately preserve inner products between sparse vectors.

Lemma 2. *Let $\mathbf{u}, \mathbf{v} \in \mathbb{R}^N$ be given, and suppose that a matrix \mathbf{A} satisfies the RIP of order $\max(\|\mathbf{u} + \mathbf{v}\|_0, \|\mathbf{u} - \mathbf{v}\|_0)$ with isometry constant δ . Then*

$$|\langle \mathbf{A}\mathbf{u}, \mathbf{A}\mathbf{v} \rangle - \langle \mathbf{u}, \mathbf{v} \rangle| \leq \delta \|\mathbf{u}\|_2 \|\mathbf{v}\|_2. \quad (22)$$

Proof. We first assume that $\|\mathbf{u}\|_2 = \|\mathbf{v}\|_2 = 1$. From the fact that

$$\|\mathbf{u} \pm \mathbf{v}\|_2^2 = \|\mathbf{u}\|_2^2 + \|\mathbf{v}\|_2^2 \pm 2\langle \mathbf{u}, \mathbf{v} \rangle = 2 \pm 2\langle \mathbf{u}, \mathbf{v} \rangle$$

and since \mathbf{A} satisfies the RIP, we have that

$$(1-\delta)(2 \pm 2\langle \mathbf{u}, \mathbf{v} \rangle) \leq \|\mathbf{A}\mathbf{u} \pm \mathbf{A}\mathbf{v}\|_2^2 \leq (1+\delta)(2 \pm 2\langle \mathbf{u}, \mathbf{v} \rangle).$$

From the parallelogram identity we obtain

$$\langle \mathbf{A}\mathbf{u}, \mathbf{A}\mathbf{v} \rangle = \frac{1}{4} (\|\mathbf{A}\mathbf{u} + \mathbf{A}\mathbf{v}\|_2^2 - \|\mathbf{A}\mathbf{u} - \mathbf{A}\mathbf{v}\|_2^2) \quad (23)$$

$$\leq \frac{(1 + \langle \mathbf{u}, \mathbf{v} \rangle)(1 + \delta) - (1 - \langle \mathbf{u}, \mathbf{v} \rangle)(1 - \delta)}{2} = \langle \mathbf{u}, \mathbf{v} \rangle + \delta. \quad (24)$$

Similarly, one can show that $\langle \mathbf{A}\mathbf{u}, \mathbf{A}\mathbf{v} \rangle \geq \langle \mathbf{u}, \mathbf{v} \rangle - \delta$, and thus $|\langle \mathbf{A}\mathbf{u}, \mathbf{A}\mathbf{v} \rangle - \langle \mathbf{u}, \mathbf{v} \rangle| \leq \delta$. The result follows for \mathbf{u}, \mathbf{v} with arbitrary norm from the bilinearity of the inner product. \square

One consequence of this result is that sparse vectors that are orthogonal in \mathbb{R}^N remain nearly orthogonal after the application of \mathbf{A} . From this observation, it was demonstrated independently in [22] and [17] that if \mathbf{A} has the RIP, then $\mathbf{P}_\Lambda^\perp \mathbf{A}$ satisfies a modified version of the RIP.

Theorem 3. *Suppose that \mathbf{A} satisfies the RIP of order K with isometry constant δ , and let $\Lambda \subset \{1, 2, \dots, N\}$. Define \mathbf{P}_Λ^\perp as in (6). If $|\Lambda| < K$ then*

$$\left(1 - \frac{\delta}{1 - \delta}\right) \|\mathbf{u}\|_2^2 \leq \|\mathbf{P}_\Lambda^\perp \mathbf{A} \mathbf{u}\|_2^2 \leq (1 + \delta) \|\mathbf{u}\|_2^2 \quad (25)$$

for all $\mathbf{u} \in \mathbb{R}^N$ such that $\|\mathbf{u}\|_0 \leq K - |\Lambda|$ and $\text{supp}(\mathbf{u}) \cap \Lambda = \emptyset$.

Proof. From the definition of $\mathbf{P}_\Lambda^\perp \mathbf{A}$ in (5), we may decompose $\mathbf{P}_\Lambda^\perp \mathbf{A} \mathbf{u}$ as $\mathbf{P}_\Lambda^\perp \mathbf{A} \mathbf{u} = \mathbf{A} \mathbf{u} - \mathbf{P}_\Lambda \mathbf{A} \mathbf{u}$. Since \mathbf{P}_Λ is an orthogonal projection, we can write

$$\|\mathbf{A} \mathbf{u}\|_2^2 = \|\mathbf{P}_\Lambda \mathbf{A} \mathbf{u}\|_2^2 + \|\mathbf{P}_\Lambda^\perp \mathbf{A} \mathbf{u}\|_2^2. \quad (26)$$

Our goal is to show that $\|\mathbf{A} \mathbf{u}\|_2 \approx \|\mathbf{P}_\Lambda^\perp \mathbf{A} \mathbf{u}\|_2$, or equivalently, that $\|\mathbf{P}_\Lambda \mathbf{A} \mathbf{u}\|_2$ is small. Towards this end, we note that since $\mathbf{P}_\Lambda \mathbf{A} \mathbf{u}$ is orthogonal to $\mathbf{P}_\Lambda^\perp \mathbf{A} \mathbf{u}$, we have

$$\begin{aligned} \langle \mathbf{P}_\Lambda \mathbf{A} \mathbf{u}, \mathbf{A} \mathbf{u} \rangle &= \langle \mathbf{P}_\Lambda \mathbf{A} \mathbf{u}, \mathbf{P}_\Lambda \mathbf{A} \mathbf{u} + \mathbf{P}_\Lambda^\perp \mathbf{A} \mathbf{u} \rangle \\ &= \langle \mathbf{P}_\Lambda \mathbf{A} \mathbf{u}, \mathbf{P}_\Lambda \mathbf{A} \mathbf{u} \rangle + \langle \mathbf{P}_\Lambda \mathbf{A} \mathbf{u}, \mathbf{P}_\Lambda^\perp \mathbf{A} \mathbf{u} \rangle \\ &= \|\mathbf{P}_\Lambda \mathbf{A} \mathbf{u}\|_2^2. \end{aligned} \quad (27)$$

Since \mathbf{P}_Λ is a projection onto $\mathcal{R}(\mathbf{A}_\Lambda)$ there exists a $\mathbf{z} \in \mathbb{R}^N$ with $\text{supp}(\mathbf{z}) \subseteq \Lambda$ such that $\mathbf{P}_\Lambda \mathbf{A} \mathbf{u} = \mathbf{A} \mathbf{z}$. Furthermore, by assumption, $\text{supp}(\mathbf{u}) \cap \Lambda = \emptyset$. Hence $\langle \mathbf{u}, \mathbf{z} \rangle = 0$ and from the RIP and Lemma 2,

$$\frac{|\langle \mathbf{P}_\Lambda \mathbf{A} \mathbf{u}, \mathbf{A} \mathbf{u} \rangle|}{\|\mathbf{P}_\Lambda \mathbf{A} \mathbf{u}\|_2 \|\mathbf{A} \mathbf{u}\|_2} = \frac{|\langle \mathbf{A} \mathbf{z}, \mathbf{A} \mathbf{u} \rangle|}{\|\mathbf{A} \mathbf{z}\|_2 \|\mathbf{A} \mathbf{u}\|_2} \leq \frac{|\langle \mathbf{A} \mathbf{z}, \mathbf{A} \mathbf{u} \rangle|}{(1 - \delta) \|\mathbf{z}\|_2 \|\mathbf{u}\|_2} \leq \frac{\delta}{1 - \delta}.$$

Combining this with (27), we obtain

$$\|\mathbf{P}_\Lambda \mathbf{A} \mathbf{u}\|_2 \leq \frac{\delta}{1 - \delta} \|\mathbf{A} \mathbf{u}\|_2.$$

Since we trivially have that $\|\mathbf{P}_\Lambda \mathbf{A} \mathbf{u}\|_2 \geq 0$, we can combine this with (26) to obtain

$$\left(1 - \left(\frac{\delta}{1 - \delta}\right)^2\right) \|\mathbf{A} \mathbf{u}\|_2^2 \leq \|\mathbf{P}_\Lambda^\perp \mathbf{A} \mathbf{u}\|_2^2 \leq \|\mathbf{A} \mathbf{u}\|_2^2.$$

Since $\|\mathbf{u}\|_0 \leq K$, we can use the RIP to obtain

$$\left(1 - \left(\frac{\delta}{1 - \delta}\right)^2\right) (1 - \delta) \|\mathbf{u}\|_2^2 \leq \|\mathbf{P}_\Lambda^\perp \mathbf{A} \mathbf{u}\|_2^2 \leq (1 + \delta) \|\mathbf{u}\|_2^2,$$

which simplifies to (25). □

References

- [1] E. Candès, “Compressive sampling,” in *Proc. Int. Congress Math.*, Madrid, Spain, Aug. 2006.
- [2] D. Donoho, “Compressed sensing,” *IEEE Trans. Inform. Theory*, vol. 6, no. 4, pp. 1289–1306, 2006.
- [3] R. Baraniuk, M. Davenport, R. DeVore, and M. Wakin, “A simple proof of the restricted isometry property for random matrices,” *Const. Approx.*, vol. 28, no. 3, pp. 253–263, 2008.
- [4] A. Calderbank and I. Daubechies, “The pros and cons of democracy,” *IEEE Trans. Inform. Theory*, vol. 48, no. 6, 2002.
- [5] S. Güntürk, *Harmonic analysis of two problems in signal compression*, Ph.D. thesis, Program in Applied and Computation Mathematics, Princeton University, Princeton, NJ, Sept. 2000.
- [6] E. Candès, “Integration of sensing and processing,” *IMA Annual Program Year Work.*, Dec. 2005.
- [7] J. Romberg and M. Wakin, “Compressed sensing: A tutorial,” *IEEE Work. Stat. Signal Processing (SSP)*, Aug. 2007.
- [8] J. Laska, P. Boufounos, M. Davenport, and R. Baraniuk, “Democracy in action: Quantization, saturation, and compressive sensing,” *Preprint*, 2009.
- [9] E. Candès and T. Tao, “Decoding by linear programming,” *IEEE Trans. Inform. Theory*, vol. 51, no. 12, pp. 4203–4215, 2005.
- [10] R. DeVore, G. Petrova, and P. Wojtaszczyk, “Instance-optimality in probability with an ℓ_1 -minimization decoder,” *Appl. Comput. Harmon. Anal.*, vol. 27, no. 3, pp. 275–288, 2009.
- [11] E. Candès, “The restricted isometry property and its implications for compressed sensing,” *Comptes rendus de l’Académie des Sciences, Série I*, vol. 346, no. 9-10, pp. 589–592, 2008.
- [12] T. Cai, X. Guangwu, and J. Zhang, “On recovery of sparse signals via ℓ_1 minimization,” *IEEE Trans. Inform. Theory*, vol. 55, no. 7, pp. 3388–3397, 2009.
- [13] M. Davenport and M. Wakin, “Analysis of Orthogonal Matching Pursuit using the restricted isometry property,” *Preprint*, 2009.
- [14] D. Needell and R. Vershynin, “Uniform uncertainty principle and signal recovery via regularized orthogonal matching pursuit,” *Found. Comput. Math.*, vol. 9, no. 3, pp. 317–334, 2009.
- [15] D. Needell and R. Vershynin, “Signal recovery from incomplete and inaccurate measurements via regularized orthogonal matching pursuit,” *to appear in IEEE J. Selected Topics in Signal Processing*, 2009.
- [16] D. Needell and J. Tropp, “CoSaMP: Iterative signal recovery from incomplete and inaccurate samples,” *Appl. Comput. Harmon. Anal.*, vol. 26, no. 3, pp. 301–321, 2009.
- [17] W. Dai and O. Milenkovic, “Subspace pursuit for compressive sensing signal reconstruction,” *IEEE Trans. Inform. Theory*, vol. 55, no. 5, pp. 2230–2249, 2009.
- [18] A. Cohen, W. Dahmen, and R. DeVore, “Instance optimal decoding by thresholding in compressed sensing,” *Preprint*, 2008.
- [19] T. Blumensath and M. Davies, “Iterative hard thresholding for compressive sensing,” *Appl. Comput. Harmon. Anal.*, vol. 27, no. 3, pp. 265–274, 2009.
- [20] R. Chartrand and V. Staneva, “Restricted isometry properties and nonconvex compressive sensing,” *Inverse Problems*, vol. 24, no. 035020, pp. 1–14, 2008.
- [21] J. Laska, M. Davenport, and R. Baraniuk, “Exact signal recovery from corrupted measurements through the pursuit of justice,” in *Proc. Asilomar Conf. on Signals Systems and Computers*, Asilomar, CA, Nov. 2009.
- [22] M. Davenport, P. Boufounos, and R. Baraniuk, “Compressive domain interference cancellation,” in *Structure et parcimonie pour la représentation adaptative de signaux (SPARS)*, Saint-Malo, France, Apr. 2009.
- [23] E. Candès, J. Romberg, and T. Tao, “Stable signal recovery from incomplete and inaccurate measurements,” *Comm. Pure and Appl. Math.*, vol. 59, no. 8, pp. 1207–1223, 2006.
- [24] S. Dasgupta and A. Gupta, “An elementary proof of the Johnson-Lindenstrauss lemma,” *Tech. Report 99-006*, U.C. Berkeley, Mar. 1999.
- [25] N. Johnson, S. Kotz, and N. Balakrishnan, *Continuous Univariate Distributions, Volume 1*, Wiley, 1994.
- [26] V. Buldygin and Y. Kozachenko, *Metric Characterization of Random Variables and Random Processes*, AMS, 2000.
- [27] M. Davenport, “Concentration of measure and sub-gaussian distributions,” 2009, Available from <http://cnx.org/content/m32583/latest/>.
- [28] G. Lorentz, M. Golitschek, and Y. Makovoz, *Constructive Approximation: Advanced Problems*, Springer-Verlag, 1996.