

# Near Optimal Signal Recovery From Random Projections: Universal Encoding Strategies?

Emmanuel Candes<sup>†</sup> and Terence Tao<sup>‡</sup>

<sup>†</sup> Applied and Computational Mathematics, Caltech, Pasadena, CA 91125

<sup>‡</sup> Department of Mathematics, University of California, Los Angeles, CA 90095

October 2004

## Abstract

Suppose we are given a vector  $f$  in  $\mathbf{R}^N$ . How many linear measurements do we need to make about  $f$  to be able to recover  $f$  to within precision  $\epsilon$  in the Euclidean ( $\ell_2$ ) metric? Or more exactly, suppose we are interested in a class  $\mathcal{F}$  of such objects—discrete digital signals, images, etc; how many linear measurements do we need to recover objects from this class to within accuracy  $\epsilon$ ?

This paper shows that if the objects of interest are sparse or compressible in the sense that the reordered entries of a signal  $f \in \mathcal{F}$  decay like a power-law (or if the coefficient sequence of  $f$  in a fixed basis decays like a power-law), then it is possible to reconstruct  $f$  to within very high accuracy from a small number of random measurements. A typical result is as follows: we rearrange the entries of  $f$  (or its coefficients in a fixed basis) in decreasing order of magnitude  $|f|_{(1)} \geq |f|_{(2)} \geq \dots \geq |f|_{(N)}$ , and define the weak- $\ell_p$  ball as the class  $\mathcal{F}$  of those elements whose entries obey the power decay law

$$|f|_{(n)} \leq C \cdot n^{-1/p}.$$

We take measurements  $\langle f, X_k \rangle$ ,  $k = 1, \dots, K$ , where the  $X_k$  are  $N$ -dimensional Gaussian vectors with independent standard normal entries, say. Then for each  $f \in \mathcal{F}$  for some  $0 < p < 1$  and with overwhelming probability, one can reconstruct an object  $f^\sharp$  from the data of these  $K$  random coefficients only, and with the property

$$\|f - f^\sharp\|_{\ell_2} \leq C_r \cdot (K/\log N)^{-r}, \quad r = 1/p - 1/2.$$

Moreover, the reconstruction can be obtained by solving a linear program which searches among all candidates  $g$  fitting the observed data, for that with minimum  $\ell_1$ -norm

$$\min_{g \in \mathbf{R}^N} \sum_{t=1}^N |g(t)|.$$

The methodology extends to various other random measurement ensembles; for example, we show that similar results hold if one observes few randomly sampled Fourier coefficients of  $f$ . Indeed, our results are quite general and require only two hypotheses on the measurement ensemble, which we call the uniform uncertainty principle property and the exact reconstruction property.

Alternatively, we can think of the random measurement process as some kind of universal encoder. The encoder essentially correlates the signal with white-noise and the decoder upon receiving such quantized random measurements, reconstruct an approximate signal by minimizing the  $\ell_1$ -norm. There is a sense in which this encoder/decoder pair asymptotically achieves nearly optimal information theoretic limits.

**Keywords.** Random matrices, singular values of random matrices, signal recovery, random projections, concentration of measure, sparsity, trigonometric expansions, uncertainty principle, convex optimization, duality in optimization, linear programming.

**Acknowledgments.** E. C. is partially supported by National Science Foundation grants DMS 01-40698 (FRG) and ACI-0204932 (ITR), and by an Alfred P. Sloan Fellowship. T. T. is supported in part by a grant from the Packard Foundation. E. C. would like to thank Justin Romberg and Houman Ohwadi for conversations related to this project, and Nouredine El Karoui for sending us an early draft of his Ph. D. thesis. T. T. thanks Wilhelm Schlag and Gerd Mockenhaupt for pointing out the relevance of Bourgain's work [4], [5].

## 1 Introduction

This paper considers the fundamental problem of recovering a finite signal  $f \in \mathbf{R}^N$  from a limited set of measurements. Specifically, given a class of signals  $\mathcal{F} \subset \mathbf{R}^N$ , one is interested in the minimum number of linear measurements one has to make to be able to reconstruct objects from  $\mathcal{F}$  to within a fixed accuracy  $\epsilon$ , say, in the usual Euclidean  $\ell_2$ -distance. In other words, how can one specify  $K = K(\epsilon)$  linear functionals

$$y_k = \langle f, \psi_k \rangle, \quad k \in \Omega, \quad (1.1)$$

where  $(\psi_k)_{k \in \Omega}$  is a set of vectors with cardinality  $|\Omega| = K$ , so that it is possible to reconstruct an object  $f^\#$  from the data  $(y_k)_{k \in \Omega}$  obeying

$$\|f - f^\#\|_{\ell_2} \leq \epsilon, \quad (1.2)$$

for typical elements  $f$  taken from  $\mathcal{F}$ ? The primary goal is of course, to find appropriate functionals  $(\psi_k)_{k \in \Omega}$  so that the required number  $K$  of measurements is as small as possible. In addition, we are also interested in concrete and practical recovery algorithms.

The new results in this paper will address this type of question for signals  $f$  whose coefficients with respect to a fixed reference basis obey a power law type decay condition, and for random measurements  $(y_k)_{k \in \Omega}$  sampled from a specified ensemble. However, before we discuss these results, we first recall some earlier results concerning signals of small support.

### 1.1 Exact Reconstruction of Sparse Signals

In a previous article [9], the authors together with J. Romberg studied the recovery of *sparse* signals from limited measurements; i.e. of signals which have relatively few nonzero terms or whose coefficients in some fixed basis have relatively few nonzero entries. This paper discussed some surprising phenomena, and we now review a special instance of those. In order to do so, we first need to introduce the discrete Fourier transform which is given

by the usual formula<sup>1</sup>

$$\hat{f}(k) := \frac{1}{\sqrt{N}} \sum_{t \in \mathbb{Z}_N} f(t) e^{-i2\pi kt/N}, \quad (1.3)$$

where the frequency index  $k$  ranges over the set  $\mathbb{Z}_N := \{0, 1, \dots, N-1\}$ .

Suppose then that we wish to recover a signal  $f \in \mathbf{R}^N$  made out of  $|T|$  spikes, where the set  $T$  denotes the support of the signal

$$T := \{t, f(t) \neq 0\}.$$

We do not know where the spikes are located nor do we know their amplitudes. However, we are given information about  $f$  in the form of 'only'  $|\Omega| \approx \tau N$  randomly sampled Fourier coefficients  $F_\Omega f := (\hat{f}(k))_{k \in \Omega}$ , where  $0 < \tau < 1$  is fixed and  $\Omega$  is the random set

$$\Omega := \{k \in \mathbb{Z}_N : I_k = 1\}, \quad (1.4)$$

where  $I_k$  are i.i.d. Bernoulli selectors with  $\mathbf{P}(I_k = 1) = \tau$ . In [9], it was shown that  $f$  could be reconstructed *exactly* from these data provided that the expected number of frequency samples obeyed the lower bound

$$|T| \leq \alpha \cdot (\mathbf{E}|\Omega| / \log N) \quad (1.5)$$

for all sufficiently small  $\alpha > 0$  (i.e.  $\alpha \leq \alpha_0$  for some small absolute constant  $\alpha_0$ ). To recover  $f$  from  $F_\Omega f$ , we simply minimize the  $\ell_1$ -norm of the reconstructed signal

$$\min \|g\|_{\ell_1} := \sum_{t \in \mathbb{Z}_N} |g(t)|, \quad (1.6)$$

subject to the constraints

$$\hat{g}(k) = \hat{f}(k) \quad \forall k \in \Omega.$$

Moreover, the probability that exact recovery occurs exceeds  $1 - O(N^{-\rho/\alpha})$ ;  $\rho > 0$  is here a universal constant and it is worth noting that the aforementioned reference gave explicit values for this constant. In short, exact recovery may be achieved by solving a simple convex optimization problem—in fact, a linear program for real-valued signals—which is a result of practical significance.

In a following paper, Candès and Romberg [10] extended these results and showed that exact reconstruction phenomena hold for other synthesis/measurement pairs. For clarity of presentation, it will be convenient to introduce some notations that we will use throughout the remainder of the paper. We let  $F_\Omega$  denote the  $|\Omega|$  by  $N$  matrix which specifies the set of those  $|\Omega|$  linear functionals which describe the measurement process so that the available information  $y$  about  $f$  is of the form

$$y = F_\Omega f.$$

For instance, in our previous example,  $F_\Omega$  is the  $|\Omega|$  by  $N$  partial Fourier matrix whose rows are the sampled sinusoids

$$F_\Omega(k, t) := \frac{1}{\sqrt{N}} e^{-i2\pi kt/N}, \quad k \in \Omega, t \in \mathbb{Z}_N.$$

---

<sup>1</sup>Strictly speaking, the Fourier transform is associated to an orthonormal basis in  $\mathbf{C}^N$  rather than  $\mathbf{R}^N$ . However all of our analysis here extends easily to complex signals instead of real signals (except for some negligible changes in the absolute constants  $C$ ). For ease of exposition we shall focus primarily on real-valued signals  $f \in \mathbf{R}^N$ , except when referring to the Fourier basis.

More generally, suppose that one is given an orthonormal basis  $\Psi$

$$\Psi = (\psi_k(t))_{0 \leq t, k < N},$$

and that one has available partial information about  $f$  in the sense that we have knowledge about a randomly selected set  $\Omega \subset \{0, \dots, N-1\}$  of coefficients in basis  $\Psi$ . For convenience, define  $F_\Omega$  to be the  $N$  by  $N$  synthesis matrix with entries  $F_\Omega(t, k) := \psi_k(t)$ . Then  $F_\Omega$  is now obtained from  $\Psi^*$  by extracting the  $|\Omega|$  rows with indices  $k$  obeying  $k \in \Omega$ . Suppose as before that there is another (fixed) orthonormal basis  $\Phi$  in which the coefficients  $\theta(f) = (\theta_t(f))_{1 \leq t \leq N}$  of  $f$  in this basis, defined by

$$\theta_t(f) := \langle f, \phi_t \rangle,$$

are sparse in the sense that only few of the entries of  $\theta(f)$  are nonzero. Then it was shown in [10] that with overwhelming probability,  $f$  is the solution to

$$\min_g \|\theta(g)\|_{\ell_1} \quad \text{subject to} \quad F_\Omega g = F_\Omega f. \quad (1.7)$$

That is, exact reconstruction still occurs; the relationship here between the number of nonzero terms in the basis  $\Phi$  and the number of observed coefficients  $|\Omega|$  depends upon the *incoherence* between the two bases. The more incoherent, the fewer coefficients needed; in the other direction, in the maximally coherent case, e.g.  $\Psi = \Phi$ , one in fact needs to sample essentially all of the coefficients in order to ensure exact reconstruction (the same holds true if  $\Phi$  and  $\Psi$  share only one element with nonzero inner product with  $f$ ).

A special instance of these results concerns the case where the set of measurements is generated completely at random; that is, we sample a random orthonormal basis of  $\mathbf{R}^N$  and observe only the first  $K$  coefficients in that basis (note that there is no advantage in randomizing  $\Omega$  as in (1.4), since the basis is already completely random). As before, we let  $F_\Omega$  be the submatrix enumerating those sampled vectors and solve (1.7). Then a consequence of the methodology developed in this paper is that exact reconstruction occurs with probability at least  $1 - O(N^{-\rho/\alpha})$  (for a different value of  $\rho$ ) provided that

$$\|\theta(f)\|_{\ell_0} \leq \alpha \cdot (K/\log N), \quad (1.8)$$

where  $\alpha > 0$  is sufficiently small, and the  $\ell_0$ -norm is of course the size of the support of the vector  $\theta$

$$\|\theta\|_{\ell_0} := |\{t : \theta_t \neq 0\}|.$$

In summary,  $\ell_1$  seems to recover sparse unknown signals in a variety of different situations. The number of measurements simply needs to exceed the number of unknown nonzero coefficients by a proper amount.

Observe that a nice feature of the random basis discussed above is its statistical invariance by rotation. Let  $\Phi$  be any basis so that  $\theta(f)$  are the coefficients of  $f$  in that basis:  $\theta(f) := \Phi^* f$ . The constraints in (1.7) impose

$$F_\Omega \Phi \theta(g) = F_\Omega \Phi \theta(f)$$

and since the distribution of  $F_\Omega \Phi$  is that of  $F_\Omega$ , the choice of the basis  $\Phi$  is actually irrelevant. Exact reconstruction occurs (with overwhelming probability) when the signal is sparse in any fixed basis; of course, the recovery algorithm requires knowledge of this basis.

## 1.2 Power laws

In general, signals of practical interest may not be supported in space or in a transform domain on a set of relatively small size. Instead, the coefficients of elements taken from a signal class decay rapidly, typically like a power-law. We now give two examples leaving mathematical rigor aside in the hope of being more concise.

- *Smooth signals.* It is well-known that if a continuous-time object has  $s$  bounded derivatives, then the  $n$ th largest entry of the wavelet or Fourier coefficient sequence is of size about  $1/n^{s+1/2}$  in one dimension and more generally,  $1/n^{s/d+1/2}$  in  $d$  dimensions. Hence, the decay of Fourier or wavelet coefficients of smooth signals exhibits a power law.
- *Signals with bounded variations* A popular model for signal/analysis is the space of objects with bounded variations. At the level of the continuum, the total-variation norm of an object is approximately the  $\ell_1$  norm of its gradient. In addition, there are obvious discrete analogs for finite signals where the gradient is replaced by finite differences. Now a norm which is almost equivalent to the total-variation norm is the weak- $\ell_1$  norm in the wavelet domain; that is, the reordered wavelet coefficients of a compactly supported object  $f$  approximately decay like  $1/n$  [17]. At the discrete level,  $\|f\|_{BV}$  essentially behaves like the  $\ell_1$ -norm of the Haar wavelet coefficients up to a multiplicative factor of at most  $\log N$ . Moreover, it is interesting to note that studies show that the empirical wavelet coefficients of photographs of natural scenes actually exhibit the  $1/n$ -decay.

In fact, finding representations with rapidly decaying coefficients is a very active area of research known as Computational Harmonic Analysis and there are of course many other such examples. For instance, certain classes of oscillatory signals have rapidly decaying Gabor coefficients [24], certain types of images with discontinuities along edges have rapidly decaying curvelet coefficients [8] and so on.

Whereas [9] considered signals  $f$  of small support, we now consider objects whose coefficients in some basis decay like a power-law. We fix an orthonormal basis  $\Phi = (\phi_t)_{1 \leq t \leq N}$  (which we call the *reference basis*), and rearrange the entries  $\theta_t(f) := \langle f, \phi_t \rangle$  of the coefficient vector  $\theta(f)$  in decreasing order of magnitude  $|\theta|_{(1)} \geq |\theta|_{(2)} \geq \dots \geq |\theta|_{(N)}$ . We say that  $\theta(f)$  belongs to the weak- $\ell_p$  ball or radius  $C$  (and we will sometimes write  $f \in w\ell_p(C)$ ) for some  $0 < p < \infty$  and  $C > 0$  if for each  $1 \leq n \leq N$ ,

$$|\theta|_{(n)} \leq C \cdot n^{-1/p}. \quad (1.9)$$

In other words,  $p$  controls the speed of the decay: the smaller  $p$ , the faster the decay. The condition (1.9) is also equivalent to the estimate

$$|\{t \in \mathbb{Z}_N : |\theta_t(f)| \geq \lambda\}| \leq \frac{C^p}{\lambda^p}$$

holding for all  $\lambda > 0$ . We shall focus primarily on the case  $0 < p < 1$ .

It is well-known that the decay rate of the coefficients of  $f$  is linked to the ‘compressibility’ of  $f$ , compare the widespread use of transform coders in the area of lossy signal or image

compression. Suppose for instance that all the coefficients  $(\theta_t(f))_{1 \leq t \leq N}$  are known and consider the partial reconstruction  $\theta_K(f)$  (where  $1 \leq K \leq N$  is fixed) obtained by keeping the  $K$  largest entries of the vector  $\theta(f)$  (and setting the others to zero). Then it immediately follows from (1.9) that the approximation error obeys

$$\|\theta(f) - \theta_K(f)\|_{\ell_2} \leq C_r \cdot K^{-r}, \quad r := 1/p - 1/2.$$

And thus, it follows from Parseval that the approximate signal  $f_K$  obtained by keeping the largest coefficients in the expansion of  $f$  in the reference basis  $\Phi$  obeys the same estimate, namely,

$$\|f - f_K\|_{\ell_2} \leq C_r \cdot K^{-r}. \quad (1.10)$$

### 1.3 Recovery of objects with power-law decay

We now return to the setup we discussed earlier, where we select  $K$  orthonormal vectors  $\psi_1, \dots, \psi_K$  in  $\mathbf{R}^N$  uniformly at random. Since applying a fixed orthonormal transform does not change the problem, we may just as well assume that  $\Phi$  is the identity and solve

$$(P_1) \quad \min_{g \in \mathbf{R}^N} \|g\|_{\ell_1} \quad \text{subject to} \quad F_\Omega g = F_\Omega f, \quad (1.11)$$

where as usual,  $F_\Omega f = (\langle f, \psi_k \rangle)_{k \in \Omega}$ . In the setting where  $f$  does not have small support, we do not expect the recovery procedure (1.11) to recover  $f$  exactly, but our first main theorem asserts that it will recover  $f$  *approximately*.

**Note.** From now on and for ease of exposition, we will take  $(P_1)$  as our abstract recovery procedure where it is understood that  $f$  is the sparse object of interest to be recovered; that is,  $f$  could be a signal in  $\mathbf{R}^N$  or its coefficients in some fixed basis  $\Phi$ .

**Theorem 1.1 (Optimal recovery of  $w_{\ell_p}$  from random measurements)** *Suppose that  $f \in \mathbf{R}^N$  obeys (1.9) for some fixed  $0 < p < 1$  or  $\|f\|_{\ell_1} \leq C$  for  $p = 1$ , and let  $\alpha > 0$  be a sufficiently small number (less than an absolute constant). Assume that we are given  $K$  random measurements  $F_\Omega f$  as described above. Then with probability 1, the minimizer  $f^\#$  to (1.11) is unique. Furthermore, we have the approximation*

$$\|f - f^\#\|_{\ell_2} \leq C_{r,\alpha} \cdot (K/\log N)^{-r}. \quad (1.12)$$

*with probability at least  $1 - O(N^{-\rho/\alpha})$ , where  $r := \frac{1}{p} - \frac{1}{2}$ , and the implicit constant in  $O(N^{-\rho/\alpha})$  is allowed to depend on  $\alpha$ .*

The result of this theorem is rather surprising. Indeed, (1.12) says that if one makes  $O(K \log N)$  random measurements of a signal  $f$ , and then reconstructs an approximate signal from this limited set of measurements in a manner which requires no prior knowledge or assumptions on the signal, *one still obtains a reconstruction error which is equally as good as that one would obtain by knowing everything about  $f$  and selecting the  $K$  largest entries of the coefficient vector  $\theta(f)$* ; thus the amount of “oversampling” incurred by this random measurement procedure compared to the optimal sampling for this level of error is only a multiplicative factor of  $O(\log N)$ . Not only that—and what is truly remarkable

here—is that the information about  $f$  can be retrieved from those random coefficients by minimizing a simple linear program (1.11).

In section 9, we will informally argue that we cannot, in general, design a set of  $K$  measurements that would allow essentially better reconstruction errors by any method, no matter how intractable. With this in mind, another striking aspect of this procedure is its adaptivity to the unknown degree of sparsity  $p$ : minimizing the  $\ell_1$ -norm gives nearly the best possible reconstruction error simultaneously over a wide range of sparse classes of signals. In other words, no prior information on the parameter  $p$  is needed to obtain an error scaling like  $(K/\log N)^{-r}$ .

As we will see later, Theorem 1.1 is a special case of Theorem 1.4 below (but for the uniqueness claim which is proved in section 3).

## 1.4 Other Measurement Ensembles

Underlying our results is a powerful machinery essentially relying on properties of random matrices which gives us very precise tools allowing to quantify how much of a signal one can reconstruct from random measurements. In fact, Theorem 1.1 holds for other *measurement ensembles*. For simplicity, we shall consider three types of measured data:

- *The Gaussian ensemble:* Here, we suppose that  $1 \leq K \leq N$  and  $\Omega := \{1, \dots, K\}$  are fixed, and the entries of  $F_\Omega$  are identically and independently sampled from a standard normal distribution

$$F_\Omega(k, t) := \frac{1}{\sqrt{N}} X_{kt}, \quad X_{kt} \text{ i.i.d. } N(0, 1).$$

The Gaussian ensemble is invariant by rotation since for any fixed orthonormal matrix  $\Phi$ , the distribution of  $F_\Omega$  is that of  $F_\Omega \Phi$ . Closely related is the renormalized model in which the rows of  $F_\Omega$  are unit-normed so that for all  $\|F_\Omega(k, \cdot)\|_{\ell_2} = 1$  or in other words, each of the  $K$  rows of  $F_\Omega$  is a properly renormalized  $N$ -dimensional vector of independent standard Gaussian random variables. Depending upon the circumstances, one may or may not impose orthogonality between the rows.

- *The binary ensemble:* Again we take  $1 \leq K \leq N$  and  $\Omega := \{1, \dots, K\}$  to be fixed. But now we suppose that the entries of  $F_\Omega$  are identically and independently sampled from a symmetric Bernoulli distribution

$$F_\Omega(k, t) := \frac{1}{\sqrt{N}} X_{kt}, \quad X_{kt} \text{ i.i.d. } P(X_{kt} = \pm 1) = 1/2.$$

- *The Fourier ensemble:* This ensemble was discussed earlier, and is obtained by randomly sampling rows from the orthonormal  $N$  by  $N$  Fourier matrix  $\mathcal{F}(k, t) = \exp(-i2\pi kt/N)/\sqrt{N}$ . Formally, we let  $0 < \tau < 1$  be a fixed parameter, and then let  $\Omega$  be the random set defined by (1.4). We then let  $R_\Omega : \ell_2(\mathbb{Z}_N) \rightarrow \ell_2(\Omega)$  be the restriction map  $(R_\Omega g)(k) = g(k)$  for all  $k \in \Omega$  (so that the adjoint  $R_\Omega^* : \ell_2(\Omega) \rightarrow \ell_2(\mathbb{Z}_N)$  is the embedding obtained by extending by zero outside of  $\Omega$ ), and set

$$F_\Omega := R_\Omega \mathcal{F}.$$

In this case, the role of  $K$  is played by the quantity  $K := \mathbf{E}(|\Omega|) = \tau N$ . (In fact  $|\Omega|$  is usually very close to  $K$ ; see Lemma 6.6).

Just as Theorem 1.1 suggests, this paper will show that it is possible to derive recovery rates for all three measurement ensembles. The ability to recover a signal  $f$  from partial random measurements depends on key properties of those measurement ensembles that we now discuss.

## 1.5 Axiomatization

We shall now unify the treatment of all these ensembles by considering an abstract *measurement matrix*  $F_\Omega$ , which is a random  $|\Omega| \times N$  matrix following some probability distribution (e.g. the Gaussian, Bernoulli, or Fourier ensembles). We also allow the number of measurements  $|\Omega|$  to also be a random variable taking variables between 1 and  $N$ , and set  $K := \mathbf{E}(|\Omega|)$  to be the expected number of measurements taken. For ease of exposition we shall restrict our attention to real-valued matrices  $F_\Omega$ ; the modifications required to cover complex matrices such as those given by the Fourier ensemble are simple. We remark that we do not assume that  $F_\Omega$  is orthogonal, although the hypothesis **UUP** that we state below can be viewed as a kind of “almost orthogonality” hypothesis on (the minors of)  $F_\Omega$ .

This section introduces two key properties on  $F_\Omega$  which—if satisfied—will guarantee that the solution to the problem (1.11) will be a good approximation to the unknown signal  $f$  in the sense of Theorem 1.1.

First, as in [9], our arguments rely, on part, on the quantitative behavior of the singular values of the matrices  $F_{\Omega T} := F_\Omega R_T^* : \ell_2(T) \rightarrow \ell_2(\Omega)$  which are the  $|\Omega|$  by  $|T|$  matrices obtained by extracting  $|T|$  columns from  $F_\Omega$  (corresponding to indices in a set  $T$ ). More precisely, we shall need to assume the following hypothesis concerning the minimum and maximum eigenvalues of the square matrix  $F_{\Omega T}^* F_{\Omega T} : \ell_2(T) \rightarrow \ell_2(T)$ .

**Definition 1.2 (UUP: Uniform Uncertainty Principle)** *We say that a measurement matrix  $F_\Omega$  obeys the uniform uncertainty principle with oversampling factor  $\lambda$  if for every sufficiently small  $\alpha > 0$ , the following statement is true with probability at least  $1 - O(N^{-\rho/\alpha})$  for some fixed positive constant  $\rho > 0$ : for all subsets  $T$  such that*

$$|T| \leq \alpha \cdot K/\lambda, \tag{1.13}$$

*the matrix  $F_{\Omega T}$  obeys the bounds*

$$\frac{1}{2} \cdot \frac{K}{N} \leq \lambda_{\min}(F_{\Omega T}^* F_{\Omega T}) \leq \lambda_{\max}(F_{\Omega T}^* F_{\Omega T}) \leq \frac{3}{2} \cdot \frac{K}{N} \tag{1.14}$$

*Note that (1.14) is equivalent to the inequality*

$$\frac{1}{2} \frac{K}{N} \|f\|_{\ell_2}^2 \leq \|F_{\Omega T} f\|_{\ell_2}^2 \leq \frac{3}{2} \frac{K}{N} \|f\|_{\ell_2}^2 \tag{1.15}$$

*holding for all signals  $f$  with small support  $|\text{supp}(f)| \leq \alpha K/\lambda$ .*

---

<sup>2</sup>We allow implicit constants in the  $O()$  notation to depend on  $\alpha$ .

To understand the content of this condition, suppose that  $F_\Omega$  is the partial Fourier transform and suppose we have a signal  $f$  with small support  $|\text{supp}(f)| \leq \alpha K/\lambda$  on a set  $T$ . Then (1.14) says that  $\|\hat{f}\|_{\ell_2(\Omega)}$  is at most  $\sqrt{3K/2N}\|f\|_{\ell_2}$  with overwhelming probability. Comparing this with Plancherel’s identity  $\|\hat{f}\|_{\ell_2(\mathbb{Z}_N)} = \|f\|_{\ell_2}$ , we see that (with overwhelming probability) a sparse signal  $f$  cannot be concentrated in frequency on  $\Omega$  *regardless of the exact support of  $f$* , unless  $K$  is comparable to  $N$ . This justifies the terminology “Uncertainty Principle”. A subtle but crucial point here is that, with overwhelming probability, we obtain the estimate (1.14) for *all* sets  $T$  obeying (1.13); this is stronger than merely asserting that each set  $T$  obeying (1.13) obeys (1.14) separately with overwhelming probability, since in the latter case the number of sets  $T$  obeying (1.13) is quite large and thus the union of all the exceptional probability events could thus also be quite large. This justifies the terminology “Uniform”. As we will see in section 3, the uniform uncertainty principle hypothesis is crucial to obtain estimates about the  $\ell_2$  distance between the reconstructed signal  $f^\#$  and the unknown signal  $f$ .

We now introduce a second hypothesis (which appears implicitly in [9], [10]) whose significance is explained below.

**Definition 1.3 (ERP: Exact Reconstruction Principle)** *We say that a measurement matrix  $F_\Omega$  obeys the exact reconstruction principle with oversampling factor  $\lambda$  if for all sufficiently small  $\alpha > 0$ , each fixed subset  $T$  obeying (1.13) and each ‘sign’ vector  $\sigma$  defined on  $T$ ,  $|\sigma(t)| = 1$ , there exists with overwhelmingly large probability a vector  $P \in \mathbf{R}^N$  with the following properties:*

- (i)  $P(t) = \sigma(t)$ , for all  $t \in T$ ;
- (ii)  $P$  is a linear combination of the rows of  $F_\Omega$  (i.e.  $P = F_\Omega^*V$  for some vector  $V$  of length  $|\Omega|$ );
- (iii) and  $|P(t)| \leq \frac{1}{2}$  for all  $t \in T^c := \{0, \dots, N-1\} \setminus T$ .

By ‘overwhelmingly large’, we mean that the probability be at least  $1 - O(N^{-\rho/\alpha})$  for some fixed positive constant  $\rho > 0$ .

**Remarks.** Section 2 will make clear that **ERP** is crucial to check that the reconstruction  $f^\#$  is close, in the  $\ell_1$ -norm, to the vector obtained by truncating  $f$ , keeping only its largest entries. Note that, in contrast to the **UUP**, in **ERP** we allow a separate exceptional event of small probability for *each* set  $T$ , rather than having a uniform event of high probability that covers all  $T$  at once. There is nothing special about the factor  $1/2$  in (iii); any quantity  $\beta$  strictly between 0 and 1 would suffice here.

To understand how **ERP** relates to our problem, suppose that  $f$  is a signal supported on a set  $T$ . Then using duality theory, it was shown in [9] that the solution to (1.11) is exact if and only if there exist a  $P$  with the above properties for  $\sigma(t) = \text{sgn}(f)(t)$ —hence the name.

**Remark.** The hypotheses **UUP** and **ERP** are closely related. For instance, one can use **UUP** to prove a statement very similar to **ERP**, but in the  $\ell_2$  norm rather than the  $\ell_\infty$  norm; see Corollary 3.1 below. One also has an implication of the form **UUP**  $\implies$  **ERP** for *generic* signals  $f$  assuming an additional weaker hypothesis **WERP**, see Section 5. In

[9] and in [10], the property **UUP** was used (together with some additional arguments) to deduce **ERP**.

We now are in position to state the main result of this paper.

**Theorem 1.4** *Let  $F_\Omega$  be a measurement process such that **UUP** and **ERP** hold with oversampling factors  $\lambda_1$  and  $\lambda_2$  respectively. Put  $\lambda = \max(\lambda_1, \lambda_2)$  and assume  $K \geq \lambda$ . Suppose that  $f$  is a signal in  $\mathbf{R}^N$  obeying (1.9) for some fixed  $0 < p < 1$  or  $\|f\|_{\ell_1} \leq C$  for  $p = 1$ , and let  $r := 1/p - 1/2$ . Then for any sufficiently small  $\alpha$ , any minimizer  $f^\sharp$  to (1.11) will obey*

$$\|f - f^\sharp\|_{\ell_2} \leq C_{r,\alpha} \cdot (K/\lambda)^{-r}. \quad (1.16)$$

with probability at least  $1 - O(N^{-\rho/\alpha})$ .

In this paper, we will show that the Gaussian and binary ensembles mentioned earlier obey **UUP** and **ERP** with  $\lambda = \log N$ , while the Fourier ensemble obeys **UUP** with  $\lambda = (\log N)^6$  and **ERP** with  $\lambda = \log N$ . Hence given an object  $f \in w\ell_p(C)$ , we prove that if we collect  $K \geq \log N$  Gaussian or binary measurements, then

$$\|f - f^\sharp\|_{\ell_2} \leq C_{r,\alpha} \cdot (K/\log N)^{-r} \quad (1.17)$$

except for a set of probability at most  $O(N^{-\rho/\alpha})$ . For randomly sampled frequency data (with at least  $(\log N)^6$  frequencies being sampled), the quality of the reconstruction now reads as

$$\|f - f^\sharp\|_{\ell_2} \leq C_r \cdot (K/(\log N)^6)^{-r}. \quad (1.18)$$

We prove this theorem in Section 3.2. Observe that our earlier Theorem 1.1 follows from (1.17) and is thus a special case of Theorem 1.4. Indeed, for a fixed  $F_\Omega$ , (1.11) is equivalent to

$$\min_g \|\theta(g)\|_{\ell_1} \quad \text{subject to} \quad P_\Omega g = P_\Omega f.$$

where  $P_\Omega$  is the orthogonal projection onto the span of the rows of  $F_\Omega$ . Now suppose as in the Gaussian ensemble that  $F_\Omega$  is a matrix with i.i.d.  $N(0, 1/N)$  entries, then  $P_\Omega$  is simply the projection onto a random plane of dimension  $K$  (with probability 1) which, of course, is the setup of Theorem 1.1.

## 1.6 About the $\ell_1$ norm

We would like to emphasize that the simple nonlinear reconstruction strategy which minimizes the  $\ell_1$ -norm subject to consistency with the measured observations is well-known in the literature of signal processing. For example in the mid-eighties, Santosa and Symes proposed this rule to reconstruct spike trains from incomplete data [39], see also [16]. We would also like to point out connections with total-variation approaches in the literature of image processing [38, 9] which are methods based on the minimization of the  $\ell_1$ -norm of the discrete gradient. Note that minimizing the  $\ell_1$ -norm is very different than standard least squares (i.e.  $\ell_2$ ) minimization procedures. With incomplete data, the least square approach would simply set to zero the 'unobserved' coefficients. Consider the Fourier case, for instance. The least-squares solution would set to zero all the unobserved frequencies, and

produce a minimizer of much smaller energy than the original signal and as is well-known, introduce a lot of artifacts.

More recently,  $\ell_1$ -minimization perhaps best known under the name of *Basis Pursuit*, has been proposed as a convex alternative to the combinatorial norm  $\ell_0$ , which simply counts the number of nonzero entries in a vector, for synthesizing signals as sparse superpositions of waveforms [14]. Interestingly, these methods provided great practical success [14, 13] and were shown to enjoy remarkable theoretical properties and to be closely related to various kinds of uncertainty principles [21, 22, 28, 11].

On the practical side and as is well-known [2], an  $\ell_1$ -norm minimization problem (for real-valued signals) can be recast as a linear program (LP) by essentially decomposing  $|x|$  into its positive and negative part,  $x = x_+ - x_-$  thus making available a wide array of ever more effective computational strategies, compare recent progress in interior point methods.

## 1.7 Applications

In many applications of practical interest, we often wish to reconstruct an object (a discrete signal, a discrete image and so on) from incomplete samples and it is natural to ask how much one can hope to recover. Actually, this work was motivated by the problem of reconstructing biomedical images from vastly undersampled Fourier data. Of special interest are problems in magnetic resonance (MR) angiography but it is expected that our methodology and algorithms will be suitable for other MR imagery, and to other acquisition techniques, such as tomography. In MR angiography, however, we observe few Fourier samples, and therefore if the images of interest are compressible in some transform domain such as in the wavelet domain for example, then  $\ell_1$ -based reconstructions might be especially well-suited.

Another application of these ideas might be to view the measurement/reconstruction procedure as a kind of lossy encoder/decoder pair where measurement process would play the role of an encoder and the linear program ( $P_1$ ) that of a decoder. We postpone this discussion to section 8.

## 1.8 Organization of the Paper

This paper is roughly divided into three parts and is organized as follows. This paper is roughly divided into three parts. The first part (sections 2 and 3), shows how **UUP** together with **ERP** give our main result, namely, Theorem 1.4. In section 2, we establish that the solution to (1.11) is in some sense stable in the  $\ell_1$ -norm, while section 3 introduces some  $\ell_2$ -theory and proves our main result. In the second part (sections 4, 5, 6 and 7), we show that all three measurement ensembles obey **UUP** and **ERP**. Section 4 studies singular values of random matrices and shows that the **UUP** holds for the Gaussian and binary ensembles. Since the strategy for the frequency ensemble is very different, it is presented in a separate section 7. In section 6, we prove that all three ensembles obey the **ERP**. Section 5 presents a weaker **ERP** which, in practice, is far easier to check. Finally and as noted above, we will argue in the third part of the paper that one can think of the random measurement process as some kind of universal encoder and briefly discuss some of its very special properties. We conclude with a discussion section (section 9) whose main purpose is to outline further work and point out connections with the work of others.

## 2 Stability in the $\ell_1$ -norm

In this section, we establish  $\ell_1$ -properties of any minimizer to the problem  $(P_1)$ , when the initial signal is mostly concentrated (in an  $\ell_1$  sense) on a small set.

**Lemma 2.1** *Assume that the measurement matrix  $F_\Omega$  obeys **ERP**. We let  $f$  be a fixed signal of the form  $f = f_0 + h$  where  $f_0$  is a signal supported on a set  $T$  whose size obeys (1.13). Then with probability at least  $1 - O(N^{-\rho/\alpha})$ , any  $\ell_1$ -minimizer (1.11) obeys*

$$\|f^\sharp \cdot 1_{T^c}\|_{\ell_1} \leq 4 \|h\|_{\ell_1}. \quad (2.1)$$

**Proof** Observe that since  $f$  is of course feasible for  $(P_1)$ , we immediately have

$$\|f^\sharp\|_{\ell_1} \leq \|f\|_{\ell_1} \leq \|f_0\|_{\ell_1} + \|h\|_{\ell_1}. \quad (2.2)$$

Now because **ERP** holds, one can construct—with the required probability—a function  $P = F_\Omega^* V$  for some  $V \in \ell_2(K)$  such that  $P = \text{sgn}(f_0)$  on  $T$  and  $|P(t)| \leq 1/2$  away from  $T$ . Observe the identity

$$\langle f^\sharp, P \rangle = \langle f^\sharp, F_\Omega^* V \rangle = \langle F_\Omega f^\sharp, V \rangle = \langle F_\Omega(f_0 + h), V \rangle = \langle f_0 + h, F_\Omega^* V \rangle = \langle f_0 + h, P \rangle.$$

Then on the one hand

$$\langle f^\sharp, P \rangle = \langle f_0, P \rangle + \langle h, P \rangle \geq \|f_0\|_{\ell_1} - \|h\|_{\ell_1},$$

while on the other hand, the bounds on  $P$  give

$$\begin{aligned} |\langle f^\sharp, P \rangle| &\leq \sum_T |f^\sharp(t)P(t)| + \sum_{T^c} |f^\sharp(t)P(t)| \\ &\leq \sum_T |f^\sharp(t)| + \frac{1}{2} \sum_{T^c} |f^\sharp(t)| \leq \sum_{\mathbb{Z}_N} |f^\sharp(t)| - \frac{1}{2} \sum_{T^c} |f^\sharp(t)|. \end{aligned}$$

To conclude, we established that

$$\|f_0\|_{\ell_1} - \|h\|_{\ell_1} \leq \|f^\sharp\|_{\ell_1} - \frac{1}{2} \|f^\sharp \cdot 1_{T^c}\|_{\ell_1},$$

and together with (2.2) proved that

$$\|f^\sharp \cdot 1_{T^c}\|_{\ell_1} \leq 4 \|h\|_{\ell_1},$$

as claimed. ■

This lemma says that any minimizer is approximately concentrated on the same set as the signal  $f$ . Indeed, suppose that  $f$  obeys (1.9) and consider  $T$  to be the set of largest values of  $|f|$ . Set  $f_0 = f \cdot 1_T$ . Then the property (1.9) gives

$$\|h\|_{\ell_1} = \|f \cdot 1_{T^c}\|_{\ell_1} \leq C_p \cdot |T|^{1-1/p}$$

for some constant  $C_p$  only depending on  $p$ , and therefore (2.1) gives

$$\|f^\sharp \cdot 1_{T^c}\|_{\ell_1} \leq 4C_p \cdot |T|^{1-1/p}. \quad (2.3)$$

Thus,  $f^\sharp$  puts 'little mass' outside of the set  $T$ .

**Corollary 2.2** *Let  $f^\sharp$  be any  $\ell_1$ -minimizer to the problem  $(P_1)$  and rearrange the entries of  $f^\sharp$  in decreasing order of magnitude  $|f^\sharp|_{(1)} \geq |f^\sharp|_{(2)} \geq \dots \geq |f^\sharp|_{(N)}$ . Under the hypotheses of Lemma 2.1, the  $m$ -th largest entry of  $f^\sharp$  obeys*

$$|f^\sharp|_{(m)} \leq C_p \cdot \frac{|T|^{1-1/p}}{m - |T|}, \quad \forall m > |T|. \quad (2.4)$$

**Proof** Suppose  $T$  is the set of  $|T|$  largest entries of  $f$  as above so that  $f^\sharp$  obeys (2.3). Denote by  $E_m$  the set of the  $m$ -largest values of the function  $f^\sharp$ . Obviously  $|E_m \cap T^c| \geq m - |T|$  and, therefore,

$$\|f^\sharp\|_{\ell_1(E_m \cap T^c)} \geq (m - |T|) \cdot |f^\sharp|_{(m)}.$$

The claim then follows from

$$\|f^\sharp\|_{\ell_1(E_m \cap T^c)} \leq \|f^\sharp\|_{\ell_1(T^c)} \leq C \cdot |T|^{1-1/p}.$$

■

### 3 Stability in the $\ell_2$ -norm

#### 3.1 Extension lemma

As essentially observed in [9], a matrix obeying (1.14)— think of it as a partial Fourier transform— allows to extend a function from a small set to all of  $\mathbb{Z}_N$  while constraining its Fourier transform to a fixed random set:

**Corollary 3.1 (Extension theorem)** *Assume that  $F_\Omega$  is a matrix obeying the uniform uncertainty principle **UUP**. Then with probability at least  $1 - O(N^{-\rho/\alpha})$  the following statement holds: for all sets  $T \subset \mathbb{Z}_N$  obeying the bound (1.14) and all functions  $f \in \ell_2(T)$ , there exists  $f^{ext} \in \ell_2(\mathbb{Z}_N)$  which*

- agrees with  $f$  on  $T$  ( $R_T f^{ext} = f$ ),
- belongs to the column space of  $F_\Omega^*$  (i.e.  $f^{ext} = F_\Omega^* V$  for some  $V \in \ell_2(\Omega)$ ),
- and furthermore, we have the  $\ell_2$  estimates

$$\|f^{ext}\|_{\ell_2(E)} \leq C \left(1 + \frac{|E|}{\alpha K/\lambda}\right)^{1/2} \|f\|_{\ell_2(T)} \quad (3.1)$$

valid for all  $E \subseteq \mathbb{Z}_N$ .

**Proof** We may assume that we are on an event such that the conclusions of **UUP** hold. In particular, from (1.14), the operator  $(F_{\Omega T}^* F_{\Omega T})$  is invertible and the inverse enjoys the operator norm bound

$$\|(F_{\Omega T}^* F_{\Omega T})^{-1}\| \leq 2N/K. \quad (3.2)$$

In the remainder of this paper and unless specified otherwise  $\|A\|$  will always be the operator norm of  $\|A\| := \sup_{\|x\|_{\ell_2}=1} \|Ax\|_{\ell_2}$ . We now set  $f^{ext}$  as in (5.1)

$$f^{ext} := F_{\Omega}^* F_{\Omega T} (F_{\Omega T}^* F_{\Omega T})^{-1} f.$$

As before, we easily verify that  $f^{ext}$  agrees with  $f$  on  $T$ , and is in the column space of  $F^*$ . Now we prove (3.1). It suffices to do so when  $|E| \leq \alpha K/\lambda$ , since the general claim then follows by decomposing larger  $E$ 's into smaller sets and then square-summing. But from (1.14), we see that  $F_{\Omega T}$  and  $F_{\Omega E}^*$  have operator norms of size at most  $\sqrt{3K/2N}$ , and the claim follows by composing these facts with (3.2).  $\blacksquare$

### 3.2 Proof of Theorem 1.4

Let  $T$  denote the set of the  $|T|$ -largest values of the function  $|f| + |f^{\sharp}|$  where  $|T|$  obeys the condition (1.13). Put  $h := (f - f^{\sharp}) 1_T$  be the restriction of  $f - f^{\sharp}$  to  $T$ . By Corollary 3.1, we can find a function  $g = F_{\Omega}^* V$  which matches  $h$  on  $T$  and obeys the estimate

$$\sum_{t \in E} |g(t)|^2 \leq C \sum_{t \in T} |f(t) - f^{\sharp}(t)|^2, \quad (3.3)$$

for all  $E$  disjoint from  $T$  of cardinality  $O(K/\lambda)$ . Here and in the rest of the proof, the constants  $C$  are allowed to depend on  $\alpha$ .

From the representation  $g = F_{\Omega}^* V$  and the constraint  $F_{\Omega} f = F_{\Omega} f^{\sharp}$  (from (1.11)), we have

$$\langle f - f^{\sharp}, g \rangle = \langle f - f^{\sharp}, F_{\Omega}^* V \rangle = \langle F_{\Omega} f - F_{\Omega} f^{\sharp}, g \rangle = 0,$$

and hence

$$\sum_{t \in \mathbb{Z}_N} (f - f^{\sharp})(t) \overline{g(t)} = 0.$$

Splitting into  $T$  and  $T^c$ , we obtain

$$\sum_{t \in T} |f - f^{\sharp}|^2(t) = - \sum_{t \in T^c} (f - f^{\sharp})(t) \overline{g(t)}. \quad (3.4)$$

Now observe that by construction of  $T$  we have

$$\|f - f^{\sharp}\|_{\ell_1(T^c)} \leq \|f\|_{\ell_1(T^c)} + \|f^{\sharp}\|_{\ell_1(T^c)} \leq C_p \cdot |T|^{1-1/p}. \quad (3.5)$$

Furthermore, it follows from our assumption about  $f$  and (2.4) that

$$\|f - f^{\sharp}\|_{\ell_{\infty}(T^c)} \leq C \cdot |T|^{-1/p}. \quad (3.6)$$

By interpolation, these last two inequalities give

$$\|f - f^{\sharp}\|_{\ell_2(T^c)} \leq C \cdot |T|^{1/2-1/p}, \quad (3.7)$$

and it remains to prove that the same bound holds over the set  $T$ .

In order to prove this fact, we enumerate  $T^c$  as  $n_1, n_2, \dots, n_{N-|T|}$  in decreasing order of magnitude of  $|f - f^{\sharp}|$ . We then group these into adjacent blocks  $B_J$  of size  $|T|$  (except

perhaps for the last one)  $B_J := \{n_j, J|T| < j \leq (J+1)|T|\}$ ,  $J = 0, 1, \dots$ . From (3.3) and Cauchy-Schwarz, we have

$$\sum_{j \in B_J} (f - f^\sharp)(n_j) \overline{g(n_j)} \leq C \cdot \|f - f^\sharp\|_{\ell_2(T)} \cdot I_J, \quad (3.8)$$

where

$$I_J := \sqrt{\sum_{j=J|T|+1}^{(J+1)|T|} |(f - f^\sharp)(n_j)|^2}.$$

Because we are enumerating the values of  $n_j$  in decreasing order, we have  $I_0 \leq |T|^{1/2} \cdot |f - f^\sharp|(n_1) \leq C \cdot |T|^{1/2-1/p}$  while for  $J \geq 1$  we have

$$I_J \leq |T|^{1/2} \cdot |f - f^\sharp|(n_{J|T|+1}) \leq |T|^{1/2} \cdot |T|^{-1} \cdot \|f - f^\sharp\|_{\ell_1(B_{J-1})},$$

In other words,

$$\sum_J I_J \leq I_0 + \sum_{J \geq 1} I_J \leq C \cdot |T|^{-r} + |T|^{-1/2} \cdot \|f - f^\sharp\|_{\ell_1(T^c)}$$

and, therefore, it follows from (3.5) that the summation of the inequality (3.8) over the blocks  $B_J$  gives

$$\sum_{t \in T^c} (f - f^\sharp)(t) \overline{g(t)} \leq C \cdot |T|^{-r} \cdot \|f - f^\sharp\|_{\ell_2(T)}.$$

Inserting this back into (3.4), we established

$$\|f - f^\sharp\|_{\ell_2(T)} \leq C \cdot |T|^{-r}.$$

This concludes the proof of Theorem 1.4.  $\blacksquare$

Note that by Cauchy-Schwarz, it follows from the proof of our Theorem that

$$\|f - f^\sharp\|_{\ell_1(T)} \leq C \cdot |T|^{1-1/p},$$

and, therefore, owing to (3.5), we also proved an  $\ell_1$  stability estimate

$$\|f - f^\sharp\|_{\ell_1} \leq C \cdot |T|^{1-1/p}. \quad (3.9)$$

**Remark.** Had we taken the weak- $\ell_1$  norm when  $p = 1$ , there would be a logarithmic divergence in the argument from the failure of weak  $\ell_1$  to control  $\ell_1$ , which is needed to establish (3.5). This is the reason why we required  $\ell_1$  in the hypothesis of Theorem 1.4 and showed that we also have a near-optimal signal recovery result for the unit ball of  $\ell_1$  with no additional losses (logarithmic or otherwise).

### 3.3 Uniqueness of the minimizer for the Gaussian ensemble

The claim that the minimizer  $f^\sharp$  is unique with probability 1, for Gaussian measurements, can be easily established as follows. The claim is trivial for  $f \equiv 0$  so we may assume  $f$  is not identically zero. Then  $F_\Omega f$  is almost surely non-zero. Furthermore, if one considers

each of the (finitely many) facets of the unit ball of  $\ell_1(\mathbb{Z}_N)$ , we see that with probability 1 the random Gaussian matrix  $F_\Omega$  has maximal rank on each of these facets (i.e. the image of each facet under  $F_\Omega$  has dimension equal to either  $K$  or the dimension of the facet, whichever is smaller). From this we see that every point on the boundary of the image of the unit  $\ell_1$ -ball under  $F_\Omega$  arises from a unique point on that ball. Similarly for non-zero dilates of this ball. Thus the solution to the problem (1.11) is unique as claimed.

We remark that the question of establishing uniqueness with high probability for discretely randomized ensembles such as the binary and Fourier ensembles discussed below is an interesting one, but one which we will not pursue here.

## 4 Eigenvalues of random matrices

In this section, we show that all three ensembles obey the uniform uncertainty principle **UUP**.

### 4.1 The Gaussian ensemble

Let  $X$  be an  $n$  by  $p$  matrix with i.i.d. entries sampled from the standard normal distribution. For simplicity, we assume that  $p \leq n$ . We are interested in the singular values of  $X/\sqrt{n}$  or the eigenvalues of  $X^*X/n$ . A famous result due to Marchenko and Pastur [33] states that the eigenvalues of  $X^*X/n$  have a deterministic limit distribution supported by the interval  $[(1 - \sqrt{c})^2, (1 + \sqrt{c})^2]$  as  $n, p \rightarrow \infty$ , with  $p/n \rightarrow c < 1$ . In fact, results from [41] show that the smallest (resp. largest) eigenvalue converges a.s. to  $(1 - \sqrt{c})^2$  (resp.  $(1 + \sqrt{c})^2$ ). In other words, the smallest singular value of  $X/\sqrt{n}$  converges a.s. to  $1 - \sqrt{c}$  and the largest to  $1 + \sqrt{c}$ . In addition, there are remarkably fine statements concerning the speed of the convergence of the largest singular value [29].

To study the concentration of the singular values of  $X$ , we follow an approach proposed by Ledoux [31] which makes a simple use of the concentration property, see also [23]. We let  $\lambda$  be the mapping that associates to a matrix  $X$  the ordered list of its singular values

$$\begin{aligned} \lambda : \mathbf{R}^{np} &\rightarrow \mathcal{S} := \{\lambda_1 \leq \dots \leq \lambda_p : \lambda_i \geq 0\} \\ \lambda(X) &\mapsto (\lambda_1(X), \dots, \lambda_p(X)). \end{aligned}$$

Equip  $\mathbf{R}^{np}$  with the Frobenius norm

$$\|X\|_F^2 := \text{Tr}(X^*X) = \sum_{i,j=1}^p |X_{ij}|^2$$

(the Euclidean norm over  $\mathbf{R}^{np}$ ), and  $\mathcal{S}$  with the Euclidean norm  $\|\cdot\|_{\ell_2}$ . Then the mapping  $\lambda$  is 1-Lipschitz in the sense that

$$\|\lambda(X) - \lambda(X')\|_{\ell_2} \leq \|X - X'\|_F$$

for all pairs  $(X, X')$  of  $n$  by  $p$  matrices. Further, the function  $g$  that extracts the last entry in the sequence  $\lambda_1 \leq \dots \leq \lambda_p$  is also 1-Lipschitz and, therefore,  $\lambda_{\max}(X) = g \circ \lambda(X)$  is also

1-Lipschitz. A classical application of the concentration inequality for Gaussian measures [31] then gives

$$\mathbf{P}(\lambda_{\max}(X) - m(\lambda_{\max}(X)) \geq r) \leq e^{-r^2/2}, \quad (4.1)$$

where  $m(\lambda_{\max}(X))$  is either the mean or the median of  $\lambda_{\max}(X)$ . Applying a simple rescaling shows that

$$\mathbf{P}(\lambda_{\max}(X/\sqrt{n}) - m(\lambda_{\max}(X/\sqrt{n})) \geq r) \leq e^{-nr^2/2}. \quad (4.2)$$

Of course, a similar equality also holds for the minimum singular value since the  $g$  extracting the first entry in the sequence  $\lambda_1 \leq \dots \leq \lambda_p$  is also 1-Lipschitz, and we also have

$$\mathbf{P}(\lambda_{\min}(X/\sqrt{n}) - m(\lambda_{\min}(X/\sqrt{n})) \leq -r) \leq e^{-nr^2/2}. \quad (4.3)$$

The Marchenko-Pastur law gives  $m(\lambda_{\min}(X/\sqrt{n})) \approx 1 - \sqrt{p/n}$ , and  $m(\lambda_{\max}(X/\sqrt{n})) \approx 1 + \sqrt{p/n}$ . In fact, for each  $\epsilon_0$ , and  $n$  sufficiently large, the following inequality holds

$$\mathbf{P}\left(\lambda_{\min}(X/\sqrt{n}) - (1 - \sqrt{p/n} - \epsilon_0) \leq -r\right) \leq e^{-nr^2/2}. \quad (4.4)$$

and likewise for the largest singular value  $\lambda_{\max}(X/\sqrt{n})$ . For concrete values of  $\epsilon_0$ , see [23].

As we emphasized earlier, such inequalities about the concentration of the largest and smallest singular values of Gaussian matrices have been known for at least a decade or so, and we merely presented the main ideas for expository purposes. To the best of our knowledge, the estimates presented here follow from the work of Szarek [42], see also [15]. In [32], the reader will find a more detailed discussion of such results together with many extensions and generalizations.

**Lemma 4.1** *The Gaussian ensemble obeys the uniform uncertainty principle UUP with oversampling factor  $\lambda = \log N$ .*

**Proof** Fix  $K \geq \log N$  and let  $\Omega := \{1, \dots, K\}$ . Let  $T$  be a fixed index set and let the event  $A_T$  be defined as

$$A_T := \{\|F_{\Omega T}^* F_{\Omega T}\| < K/2N\} \cup \{\|F_{\Omega T}^* F_{\Omega T}\| > 3K/2N\}.$$

It follows from the above analysis that for each  $|T|$  with  $|T| \leq |K|/2$ , say,  $\mathbf{P}(A_T)$  is at most  $O(\exp(-c|K|))$  for some  $c > 0$ . We now examine the tightness of the spectrum over all sets  $T$  with  $|T| \leq m < N/2$ . We have,

$$\begin{aligned} \mathbf{P}(\cup_{T:|T|<m} A_T) &\leq C \cdot e^{-c|K|} \cdot |\{T : |T| < m\}| \\ &\leq C \cdot e^{-c|K|} \cdot \sum_{k=1}^m \binom{N}{k} \leq C \cdot e^{-c|K|} \cdot m \cdot \binom{N}{m}. \end{aligned}$$

From Stirling's approximation  $\log n! = n \log n - n + O(\log n)$  we have the well-known formula

$$\log \binom{N}{m} = NH(m/N) + O(\log N),$$

where for  $0 < q < 1$ ,  $H$  is the entropy function

$$H(q) := -q \log q - (1 - q) \log(1 - q).$$

We plug this approximation and together with the fact that  $-(1-q)\log(1-q) \leq q$  on the one hand and  $m \leq N$  on the other, this gives

$$m \cdot \binom{N}{m} = \exp(m(\log(N/m) + 1) + O(\log N)).$$

Therefore, if  $|K| \gg \log N$ ,

$$\mathbf{P}(\cup_{T:|T|<m} A_T) \leq C \cdot \exp(-\rho|K|)$$

provided that  $m(\log(N/m) + 1) \leq (c - \rho)|K|$ . This is what we needed to establish.  $\blacksquare$

## 4.2 The binary ensemble

The analysis is nearly the same in the case where the matrix  $X$  is an  $n$  by  $p$  array with i.i.d. symmetric Bernoulli entries taking on values in  $\{-1, 1\}$ . Indeed, just as there is a concentration function for i.i.d. Gaussian random variables, there is another concentration function for i.i.d. Bernoulli variables. Specifically, (4.3) now becomes

$$\mathbf{P}(\lambda_{\min}(X/\sqrt{n}) - m(\lambda_{\min}(X/\sqrt{n})) \leq r) \leq e^{-nr^2/16}$$

and similarly for (4.2), see [31] or [23], for example. Now the singular values still exhibit the same behavior; that is  $\lambda_{\min}(X/\sqrt{n})$  and  $\lambda_{\max}(X/\sqrt{n})$  converge a.s. to  $1 - \sqrt{c}$  and  $1 + \sqrt{c}$  respectively, as  $n, p \rightarrow \infty$  with  $p/n \rightarrow c$ . As a consequence, for each  $\epsilon_0$  and  $n$  sufficiently large, one can show that the medians belong to the fixed interval  $[1 - \sqrt{p/n} - \epsilon_0, 1 + \sqrt{p/n} + \epsilon_0]$  which gives

$$\mathbf{P}(\lambda_{\min}(X/\sqrt{n}) - (1 - \sqrt{p/n} - \epsilon_0) \leq -r) \leq e^{-nr^2/16}, \quad (4.5)$$

and likewise for the largest singular value. Again, this is a fairly well-established result. For example, the work of Litvak et al. contains many results of this type which include versions of (4.5), compare Theorem 3.1 in [32].

Just as (4.4) implied the uniform uncertainty principle **UUP** for Gaussian matrices, (4.5) gives the same conclusion for the binary ensemble.

**Lemma 4.2** *The binary ensemble obeys the uniform uncertainty principle **UUP** with oversampling factor  $\lambda = \log N$ .*

The proof is of course identical to that of lemma 4.1 and is omitted.

## 4.3 The Fourier ensemble

The analysis for the Fourier ensemble is much more delicate than that for the Gaussian and binary cases, in particular requiring entropy arguments as used for instance by Bourgain [4], [5]. We prove the following lemma in the separate section 7.

**Lemma 4.3** *The Fourier ensemble obeys the uniform uncertainty principle **UUP** with oversampling factor  $\lambda = (\log N)^6$ .*

The exponent of 6 can almost certainly be lowered, but we will not attempt to seek the optimal exponent of  $\log N$  here.

## 5 Generic signals and the weak ERP

In some cases, it might be difficult to prove that the exact reconstruction principle **ERP** holds, and it is interesting to observe that **UUP** actually implies **ERP** for 'generic' sign functions  $\sigma = \pm 1$  supported on a small set  $T$ . More precisely, if we fix  $T$  and define  $\sigma$  to be supported on  $T$  with the i.i.d. Bernoulli distribution (independently of  $F_\Omega$ ), thus

$$\mathbf{P}(\sigma(t) = \pm 1) = 1/2, \quad \text{for all } t \in T.$$

then we shall construct a  $P$  obeying the conditions (i)-(iii) in the definition of **ERP**. Indeed, we shall construct  $P$  explicitly as

$$P := F_\Omega^* F_{\Omega T} (F_{\Omega T}^* F_{\Omega T})^{-1} R_T \sigma; \quad (5.1)$$

one can view this choice of  $P = F_\Omega^* V$  as the unique solution to (i) and (ii) which minimizes the  $\ell_2$  norm of  $V$ , and can thus be viewed as a kind of least-squares extension of  $\sigma$  using the rows of  $F_\Omega$ .

It is immediate to check that  $P$  obeys (i) and (ii) above. Indeed, the restriction of  $P$  to  $T$  is given by

$$R_T P = R_T F_\Omega^* F_{\Omega T} (F_{\Omega T}^* F_{\Omega T})^{-1} R_T \sigma = F_{\Omega T}^* F_{\Omega T} (F_{\Omega T}^* F_{\Omega T})^{-1} R_T \sigma = R_T \sigma$$

and, therefore, (i) is verified. Further, it follows from the definition that  $P$  is a linear combination of the columns of  $F^*$  and thus, (ii) holds. Therefore, we only need to check that for all  $t \in T^c$ ,  $|P(t)| \leq \frac{1}{2}$  with sufficiently high probability. In order to do this, we rewrite  $P(t)$  as

$$P(t) = \langle W_t, R_T \sigma \rangle,$$

where for each  $t \in T^c$ ,  $W_t$  is the  $|T|$  dimensional vector

$$W_t := (F_{\Omega T}^* F_{\Omega T})^{-1} F_{\Omega T}^* F_t$$

and  $F_t$  is the  $t^{\text{th}}$  column of  $F_\Omega$ . We now introduce another condition which is far easier to check than **ERP**.

**WERP (Weak ERP).** *We say the measurement process obeys the weak **ERP**, if for each fixed  $T$  obeying (1.13) and any  $0 < \gamma \leq 1$ ,  $F_\Omega$  obeys*

$$\|F_{\Omega T}^* F_t\|_{\ell_2} \leq \gamma \cdot \sqrt{K |T|} / N \quad \text{for all } t \in T^c \quad (5.2)$$

*with probability at least  $1 - O(N^{-\rho/\gamma})$  for some fixed positive constant  $\rho > 0$ .*

For example, it is an easy exercise in large deviation theory to show that **WERP** holds for Gaussian and binary measurements. One can also check that **WERP** holds for random frequency samples. We omit the proof of these facts, however, since we will show the stronger version, namely, **ERP** in all three cases. Instead, we would like to emphasize that **UUP** together with **WERP** actually imply **ERP** for most sign patterns  $\sigma$ .

We begin by recalling the classical Hoeffding inequality: let  $X_1, \dots, X_N = \pm 1$  be independent symmetric Bernoulli random variables and consider the sum  $S = \sum_{j=1}^N a_j X_j$ . Then

$$P(|S| \leq \lambda) \leq 2 \exp \left( -\frac{\lambda^2}{2 \|a\|_{\ell_2}^2} \right). \quad (5.3)$$

Suppose now that the  $\sigma(t)$ 's are independent Bernoulli, and independent from  $F$ . Then (5.3) gives

$$\mathbf{P}(|P(t)| > \lambda \mid \|W_t\|_{\ell_2} = \rho) \leq 2 \exp\left(-\frac{\lambda^2}{2\rho^2}\right).$$

If we now assume that both **UUP** and **WERP** hold, then for any  $0 < \gamma \leq 1$  we have

$$\|W_t\|_{\ell_2} \leq \|(F_{\Omega T}^* F_{\Omega T})^{-1}\| \cdot \|F_{\Omega T}^* F_t\|_{\ell_2} \leq 2\gamma \cdot \sqrt{\frac{|T|}{K}}.$$

with probability at least  $1 - O(N^{-\rho/\gamma})$ . This shows that

$$\begin{aligned} \mathbf{P}(|P(t)| > \lambda) &\leq \mathbf{P}\left(|P(t)| > \lambda \mid \|W_t\|_{\ell_2} \leq 2\gamma \cdot \sqrt{|T|/K}\right) + \mathbf{P}\left(\|W_t\|_{\ell_2} > 2\gamma \cdot \sqrt{|T|/K}\right) \\ &\leq 2 \exp\left(-\frac{\lambda^2}{8\gamma^2} \frac{K}{|T|}\right) + O(N^{-\rho/\gamma}) = 2e^{-\rho_0 K/|T|} + O(N^{-\rho/\gamma}). \end{aligned}$$

Hence, if  $|T| \leq \alpha K / \log N$ , then

$$\mathbf{P}\left(\sup_{t \in T^c} |P(t)| > 1/2\right) \leq O(N \cdot N^{-\rho_0/\alpha}) + O(N^{-\rho/\alpha}).$$

Therefore, if  $\alpha$  is chosen small enough, then for some small  $\rho' > 0$

$$\mathbf{P}\left(\sup_{t \in T^c} |P(t)| > 1/2\right) = O(N^{-\rho'/\alpha}).$$

In other words, **ERP** holds for most sign patterns  $\sigma$ . That is, if one is only interested in providing good reconstruction to nearly all signals (but not all) in the sense discussed above, then it is actually sufficient to check that both conditions **UUP** and **WERP** are valid.

## 6 About the exact reconstruction principle

In this section, we show that all the three ensembles obey the exact reconstruction principle **ERP**.

### 6.1 The Gaussian ensemble

To show that there is function  $P$  obeying the conditions (i)-(iii) in the definition of **ERP**, we take an approach that resembles that of section 5, and establish that  $P$  defined as in (5.1),

$$P := F_{\Omega}^* F_{\Omega T} (F_{\Omega T}^* F_{\Omega T})^{-1} R_T \sigma$$

obeys the three conditions (i)-(iii).

We already argued that  $P$  obeys (i) and (ii). Put  $P^c = R_{T^c} P$  to be the restriction of  $P$  to  $T^c$ . We need to show that

$$\sup_{T^c} |P^c(t)| \leq 1/2$$

with high probability. Begin by factorizing  $P^c$  as

$$P^c = F_{\Omega T^c}^* V, \text{ where } V := (F_{\Omega T}^* F_{\Omega T})^{-1} R_T \sigma.$$

The crucial observation is that the random matrix  $F_{\Omega T^c}^*$  and the random variable  $V$  are independent since they are functions of disjoint sets of independent variables.

**Proposition 6.1** *Conditional on  $V$ , the components of  $P^c$  are i.i.d. Gaussian with*

$$P^c(t) \sim N(0, \|V\|^2/N).$$

**Proof** Suppose  $V$  is fixed. By definition,

$$P^c(t) = \frac{1}{\sqrt{N}} \sum_{k \in \Omega} X_{k,t} V_k$$

and, therefore, it follows from the independence between the  $X_{k,t}$ 's and  $V$  for each  $t \in T^c$  that the conditional distribution of  $P^c(t)$  is normal with mean 0 and variance  $\|V\|_{\ell_2}^2/N$ . The independence between the components of  $P^c$  is a simple consequence of the independence between the columns of  $F$ .  $\blacksquare$

**Lemma 6.2** *Let  $\alpha > 0$  be sufficiently small, and suppose that  $|T|$  is chosen as in (1.13) so that **UUP** holds. The components of  $P^c(t)$  obey*

$$\mathbf{P}(|P^c(t)| > \lambda) \leq \mathbf{P}\left(|Z| > \lambda \cdot \sqrt{K/6|T|}\right) + O(N^{-\rho/\alpha}).$$

where  $Z \sim N(0, 1)$  is a standard normal random variable.

**Proof** Observe that

$$\|V\|_{\ell_2} \leq \|F_T\| \cdot \|(F_T^* F_T)^{-1}\| \cdot \|R_T \sigma\|_{\ell_2}.$$

On the event such that the conclusions of **UUP** holds,  $\|F_T\| \leq \sqrt{3K/2N}$  and also  $\|(F_T^* F_T)^{-1}\| \leq 2N/K$ . Since  $\|R_T \sigma\|_{\ell_2} = \sqrt{|T|}$ , this gives

$$\|V\|_{\ell_2} \leq \sqrt{\frac{6N \cdot |T|}{K}}.$$

Therefore,

$$\mathbf{P}(|P^c(t)| > \lambda) \leq \mathbf{P}\left(|P^c(t)| > \lambda \mid \|V\|_{\ell_2} \leq \sqrt{6N|T|/K}\right) + \mathbf{P}\left(\|V\|_{\ell_2} > \sqrt{6N|T|/K}\right).$$

The first term is bounded by Proposition 6.1 while the second is bounded via the uniform uncertainty principle **UUP**. This establishes the lemma.  $\blacksquare$

The previous lemma showed that for  $|T| \leq \alpha \cdot K/\log N$ ,

$$\mathbf{P}\left(\sup_{t \in T^c} |P^c(t)| > 1/2\right) \leq N \cdot \mathbf{P}\left(|Z| > \frac{1}{2} \sqrt{\frac{\log N}{6\alpha}}\right) + O(N^{-\rho/\alpha}) \leq 2N^{1-1/(48\alpha)} + O(N^{-\rho/\alpha}).$$

Therefore, if  $\alpha$  is chosen small enough, then for some small  $\rho' > 0$

$$\mathbf{P}\left(\sup_{t \in T^c} |P^c(t)| > 1/2\right) = O(N^{-\rho'/\alpha}).$$

In short, we proved:

**Lemma 6.3** *The Gaussian ensemble obeys the exact reconstruction principle **ERP** with oversampling factor  $\lambda = \log N$ .*

## 6.2 The binary ensemble

The strategy in the case where the entries of  $F$  are independent Bernoulli variables is nearly identical and we only discuss the main differences. Define  $P$  and  $V$  as above; obviously,  $F_{\Omega T^c}^*$  and  $V$  are still independent.

**Proposition 6.4** *Conditional on  $V$ , the components of  $P^c$  are independent and obey*

$$\mathbf{P}(|P^c(t)| > \lambda \mid V) \leq 2 \exp\left(-\frac{\lambda^2 N}{2\|V\|_{\ell_2}^2}\right).$$

**Proof** The conditional independence of the components is as before. As far as the tail-bound is concerned, we observe that  $P^c(t)$  is a weighted sum of independent Bernoulli variables and the claim follows from the Hoeffding inequality (5.3).  $\blacksquare$

The rest of the argument is as before. If  $|T|$  is selected as in (1.13) such that **UUP** holds, one has

$$\mathbf{P}(|P^c(t)| > 1/2) \leq 2N^{-1/48\alpha} + O(N^{-\rho/\alpha}).$$

And, of course, identical calculations now give

**Lemma 6.5** *The binary ensemble obeys the exact reconstruction principle **ERP** with oversampling factor  $\lambda = \log N$ .*

## 6.3 The Fourier ensemble

It turns out that the exact reconstruction principle also holds for the Fourier ensemble although the argument is considerably more involved [9]. We do not reproduce the proof here but merely indicate the strategy for proving that  $P$  (defined as before) also obeys the desired bound on the complement of  $T$  with sufficiently high probability. First we remark that  $|\Omega|$  is comparable to  $K$  with high probability. To see this, recall the Bernstein's inequality [3] which states that if  $X_1, \dots, X_m$  are independent random variables with mean-zero and obeying  $|X_i| \leq c$ , then

$$\mathbf{P}\left(\left|\sum_{i=1}^N X_i\right| > \lambda\right) \leq 2 \exp\left(-\frac{\lambda^2}{2\sigma^2 + 2c\lambda/3}\right), \quad (6.1)$$

where  $\sigma^2 = \sum_{i=1}^m \text{Var}(X_i)$ . Specializing this inequality gives the following lemma which we shall need later in this paper.

**Lemma 6.6** *Let  $0 < \tau < 1$ , and for each  $k$  let  $I_k \in \{0, 1\}$  be i.i.d. random variables with  $\mathbf{P}(I_k = 1) = \tau$ . Let  $a \in \ell_2(\mathbf{Z}_N)$  be arbitrary, and set  $\sigma^2 := \tau(1 - \tau)\|a\|_{\ell_2}^2$ . Then*

$$\mathbf{P}\left(\sum_{k \in \mathbf{Z}_N} (I_k - \tau)a(k) > \lambda\right) \leq 4 \exp\left(-\frac{\lambda^2}{4(\sigma^2 + \lambda\|a\|_{\infty}/3\sqrt{2})}\right).$$

**Proof** Letting  $S$  be the sum  $\sum_{k \in \mathbf{Z}_N} (I_k - \tau)a(k)$ , the proof follows from (6.1) by simply stating that  $P(|S| > \lambda)$  is upper bounded by the sum  $P(|S_1| > \lambda/\sqrt{2}) + P(|S_2| > \lambda/\sqrt{2})$ , where  $S_1$  and  $S_2$  are the real and imaginary parts of  $S$  respectively.  $\blacksquare$

Thus the bound on the quantity  $|\sum_{k \in \mathbf{Z}_N} (I_k - \tau)a(k)|$  exhibits a Gaussian-type behavior at small thresholds  $\lambda$ , and an exponential-type behavior at large thresholds.

Recall that  $K = \mathbf{E}(|\Omega|) = N\tau$ . Applying Lemma 6.6 with  $a \equiv 1$  (so  $\sigma^2 = N\tau(1 - \tau) \sim K$ ) and  $\lambda \ll \sqrt{K}$ , one easily obtains the claim that  $|\Omega|$  is comparable to  $K$  with the desired probability, and we shall implicitly assume this comparability in the arguments which follow. Decompose  $F_{\Omega T}^* F_{\Omega T}$  as

$$F_{\Omega T}^* F_{\Omega T} = \frac{|\Omega|}{N} (I - H),$$

where  $H$  is the matrix defined by  $H(t, t') = |\Omega|^{-1} \sum_{k \in \Omega} e^{i2\pi k(t-t')}$  if  $t \neq t'$  and 0 otherwise. We then expand the inverse as a truncated Neumann series

$$(F_{\Omega T}^* F_{\Omega T})^{-1} = \frac{N}{|\Omega|} (I + H + \dots + H^n + E),$$

where  $E$  is small remainder term. This allows to express  $P^c$  as

$$P^c = \frac{N}{|\Omega|} \cdot F_{\Omega T^c}^* F_{\Omega T} \cdot (I + H + \dots + H^n + E),$$

and one can derive bounds on each individual terms so that the sum obeys the desired property. By pursuing this strategy, the following claim was proved in [9].

**Lemma 6.7** *The Fourier ensemble obeys the exact reconstruction principle **ERP** with oversampling factor  $\lambda = \log N$ .*

## 7 Uniform Uncertainty Principles for the Fourier Ensemble

In this section, we prove Lemma 4.3. The ideas here are inspired by argument sketched in [5], as well as by related arguments in [4], [34].

Fix  $\alpha > 0$ , which we shall assume to be sufficiently small. We may take  $N$  to be large depending on  $\alpha$ , as the claim is vacuous when  $N$  is bounded depending on  $\alpha$ . If  $T$  is empty then the claim is trivial, so from (1.13) we may assume that

$$K = \tau N \geq C \log^6 N \tag{7.1}$$

for some (possibly) large constant  $C$ .

We need to prove (1.14). By self-adjointness, it would suffice to show that with probability at least  $1 - O(N^{-\rho/\alpha})$

$$\left| \langle F_{\Omega T}^* F_{\Omega T} f, f \rangle_{\ell_2(T)} - \tau \|f\|_{\ell_2(T)}^2 \right| \leq \frac{1}{4} \tau \cdot \|f\|_{\ell_2(T)}^2$$

for all  $f \in \ell_2(T)$  and all  $T$  obeying (1.13), thus  $|T| \leq m$ , where

$$m := \alpha \tau N / \log^6 N. \tag{7.2}$$

In other words, we wish to show that

$$\left| \sum_{k \in \Omega} |\hat{f}(k)|^2 - \tau \|f\|_{\ell_2(T)}^2 \right| \leq \frac{1}{4} \tau \cdot \|f\|_{\ell_2(T)}^2$$

whenever  $|T| \leq m$ . From Parseval's identity, this is the same as asking that

$$\left| \sum_{k \in \mathbf{Z}_N} (I_k - \tau) |\hat{f}(k)|^2 \right| \leq \frac{1}{4} \tau \cdot \|f\|_{\ell_2(T)}^2$$

whenever  $|T| \leq m$ . Now let  $U_m \subseteq \ell_2(\mathbf{Z}_N)$  denote the set

$$U_m := \bigcup \{B_{\ell_2(E)} : E \subseteq \mathbf{Z}_N, |E| = m\} = \{f \in \ell_2(\mathbf{Z}_N) : \|f\|_{\ell_2(\mathbf{Z}_N)} \leq 1, |\text{supp}(f)| \leq m\}.$$

Then the previous goal is equivalent to showing that

$$\sup_{f \in U_m} \left| \sum_{k \in \mathbf{Z}_N} (I_k - \tau) |\hat{f}(k)|^2 \right| \leq \frac{1}{4} \tau$$

with probability at least  $1 - O(N^{-\rho/\alpha})$  for some  $\rho > 0$ . In fact we shall obtain the stronger estimate

$$\mathbf{P} \left( \sup_{f \in U_m} \left| \sum_{k \in \mathbf{Z}_N} (I_k - \tau) |\hat{f}(k)|^2 \right| > \frac{1}{4} \tau \right) = O(\exp(-\frac{1}{\beta} \log^2 N)) \quad (7.3)$$

for some constant  $\beta > 0$ .

It remains to prove (7.3). The left-hand side of (7.3) is the large deviation probability of a supremum of random sums over  $U_m$ . This type of expression can be handled by entropy estimates on  $U_m$ , as was done in [4], [5], [34]. To follow their approach, we need some notation. For any  $f \in \ell_2(\mathbf{Z}_N)$ , we let  $\hat{f}$  be its discrete Fourier transform (1.3) and define the  $X$  norm of  $f$  by

$$\|f\|_X := \sqrt{N} \cdot \|\hat{f}\|_{\ell_\infty}.$$

Intuitively, if  $f$  is a “generic” function bounded in  $\ell_2(\mathbf{Z}_N)$  we expect the  $X$  norm of  $f$  to be also bounded (by standard large deviation estimates). To formalize this intuition we shall need entropy estimates on  $U_m$  in the  $X$  norm. Let  $B_X$  be the unit ball of  $X$  in  $\ell_2(\mathbf{Z}_N)$ . Thus for instance  $U_m$  is contained inside the ball  $\sqrt{m} \cdot B_X$ , thanks to Cauchy-Schwarz. However we have much better entropy estimates available on  $U_m$  in the  $X$  norm, which we now state.

**Definition 7.1 (Kolmogorov entropy)** *Let  $X$  be a (finite-dimensional) normed vector space with norm  $\|\cdot\|_X$ , and let  $B_X := \{x \in X : \|x\|_X < 1\}$  be the unit ball of  $X$ . If  $U \subset X$  is any bounded non-empty subset of  $X$  and  $r > 0$ , we define the covering number  $N(U, B_X, r) \in \mathbf{Z}^+$  to be the least integer  $N$  such that there exist elements  $x_1, \dots, x_N \in X$  such that the balls  $x_j + rB_X = \{x \in X : \|x - x_j\|_X < r\}$ ,  $1 \leq j \leq N$  cover  $U$ , and the Kolmogorov entropy as*

$$\mathcal{E}(U, B_X, r) := \log_2(N(U, B_X, r)).$$

**Proposition 7.2** *We have*

$$\mathcal{E}(U_m, B_X, r) \leq C \cdot m \log N \cdot \min(r^{-2} \log N, 1) \quad (7.4)$$

for all  $r > N^{-2}$ .

This proposition is essentially contained in [4], [5], [34]; for sake of completeness we give a proof of the proposition in the next section. Let us assume this proposition for the moment and conclude the proof of Lemma 4.3. Let  $2^j$  be a power of two with  $N^{-2} \leq 2^j \leq \sqrt{m}$ . By (7.4) one can find a finite subset  $A_j$  of  $U_m$  of cardinality

$$|A_j| \leq \exp\left(\frac{C}{1+2^{2j}} \cdot m \log^2 N\right), \quad (7.5)$$

such that for all  $f \in U_m$ , there exists  $f_j \in A_j$  such that  $\|f - f_j\|_X \leq 2^{j+1}$ . Let us fix such sets  $A_j$ . Then for any  $f \in U_m$ , we have the telescoping decomposition

$$\hat{f}(k) = \sum_{N^{-2} \leq 2^j \leq \sqrt{m}} (\hat{f}_j(k) - \hat{f}_{j+1}(k)) + \hat{f}_{-\infty}(k)$$

where  $f_j \in A_j$ ,  $\|f_j - f_{j+1}\|_X \leq 2^{j+2}$ , and  $\|f_{-\infty}\|_X \leq N^{-1}$ ; here we have the convention that  $f_j = 0$  and  $A_j = \{0\}$  if  $2^j > \sqrt{m}$ . We write  $g_j := f_j - f_{j+1}$ . We square both sides, and use the crude estimates

$$|\hat{f}(k)| \leq \|\hat{f}\|_{\ell_2} = \|f\|_{\ell_2} = 1$$

and

$$|\hat{f}_{-\infty}(k)| = \|f_{-\infty}\|_X / \sqrt{N} \leq N^{-5/2}$$

to obtain

$$|\hat{f}(k)|^2 = \left| \sum_{N^{-2} \leq 2^j \leq \sqrt{m}} \hat{g}_j(k) \right|^2 + O(N^{-5/2}).$$

Multiplying this by  $I_k - \tau$  and summing, we obtain

$$\begin{aligned} \left| \sum_{k \in \mathbf{Z}_N} (I_k - \tau) |\hat{f}(k)|^2 \right| &= \left| \sum_{k \in \mathbf{Z}_N} (I_k - \tau) \sum_{N^{-1} \leq 2^j \leq \sqrt{m}} \hat{g}_j(k) \right|^2 + O(N^{-3/2}) \\ &\leq 2 \sum_{N^{-2} \leq 2^j \leq 2^{j'} \leq \sqrt{m}} Q(g_j, g_{j'}) + O(N^{-3/2}). \end{aligned}$$

where  $Q(g_j, g_{j'})$  is the non-negative random variable

$$Q(g_j, g_{j'}) := \left| \sum_{k \in \mathbf{Z}_N} (I_k - \tau) \operatorname{Re}(\hat{g}_j(k) \overline{\hat{g}_{j'}(k)}) \right|.$$

By (7.1), the error term  $O(N^{-3/2})$  is less than  $\tau/20$  (say) if  $N$  is sufficiently large. Thus to prove (7.3) it suffices to show that

$$\mathbf{P} \left( \sum_{N^{-2} \leq 2^j \leq 2^{j'} \leq \sqrt{m}} \sup_{g_j \in A_j - A_{j+1}} \sup_{g_{j'} \in A_{j'} - A_{j'+1}} Q(g_j, g_{j'}) > \frac{\tau}{10} \right) = O(\exp(-\frac{1}{\beta} \log^2 N)). \quad (7.6)$$

By the pigeonhole principle, we can then bound the left-hand side of (7.6) by

$$\sum_{N^{-2} \leq 2^j \leq 2^{j'} \leq \sqrt{m}} \mathbf{P} \left( \sup_{g_j \in A_j - A_{j+1}} \sup_{g_{j'} \in A_{j'} - A_{j'+1}} Q(g_j, g_{j'}) > c_{j,j'} \cdot \tau \right),$$

where the  $c_{j,j'}$ 's will be decided later and obey

$$\sum_{N^{-2} \leq 2^j \leq 2^{j'} \leq \sqrt{m}} c_{j,j'} \leq 1/10. \quad (7.7)$$

Since the number of pairs  $(j, j')$  is  $O(\log^2 N)$ , which is much smaller than  $\exp(\frac{1}{\beta} \log^2 N)$ , it now suffices to show (after adjusting the value of  $\beta$  slightly) that

$$\mathbf{P} \left( \sup_{g_j \in A_j - A_{j+1}} \sup_{g_{j'} \in A_{j'} - A_{j'+1}} Q(g_j, g_{j'}) > c_{j,j'} \cdot \tau \right) = O(\exp(-\frac{1}{\beta} \log^2 N)).$$

whenever  $N^{-2} \leq 2^j \leq 2^{j'} \leq \sqrt{m}$ .

Fix  $j, j'$  as above. From (7.5) the number of possible values of  $g_{j'}$  is at most  $\exp(\frac{C}{1+2^{2j'}} \cdot m \log N)$ . Thus by the union bound it suffices to show that

$$\mathbf{P} \left( \sup_{g_j \in A_j - A_{j+1}} Q(g_j, g_{j'}) > c_{j,j'} \cdot \tau \right) = O(\exp(-\frac{C}{1+2^{2j'}} \cdot m \log^2 N));$$

for each  $g_{j'} \in A_{j'} - A_{j'+1}$ ; note that we can absorb the  $\exp(-\frac{1}{\beta} \log^2 N)$  factor since  $2^{2j'} \leq m$ .

Fix  $g_{j'}$ . We could also apply the union bound to eliminate the supremum over  $g_j$ , but it turns out that this will lead to inferior bounds at this stage, because of the poor  $\ell_\infty$  control on  $g_{j'}$ . We have to first split the frequency domain  $\mathbf{Z}_N$  into two sets  $\mathbf{Z}_N = E_1 \cup E_2$ , where

$$E_1 := \{k \in \mathbf{Z}_N : |\hat{g}_{j'}(k)| \geq \frac{C_0 2^j}{c_{j,j'} \sqrt{N}}\} \text{ and } E_2 := \{k \in \mathbf{Z}_N : |\hat{g}_{j'}(k)| < \frac{C_0 2^j}{c_{j,j'} \sqrt{N}}\}$$

for some large absolute constant  $C_0$ . Note that these sets depend on  $g_{j'}$  but not on  $g_j$ . It thus suffices to show that

$$\mathbf{P} \left( \sup_{g_j \in A_j - A_{j+1}} Q_i(g_j, g_{j'}) > c_{j,j'} \cdot \tau \right) = O(\exp(-\frac{C}{1+2^{2j'}} \cdot m \log^2 N)) \quad (7.8)$$

for  $i = 1, 2$ , where we have substituted (7.2), and  $Q_i(g_j, g_{j'})$  is the random variable

$$Q_i(g_j, g_{j'}) := \left| \sum_{k \in E_i} (I_k - \tau) \operatorname{Re}(\hat{g}_j(k) \overline{\hat{g}_{j'}(k)}) \right|.$$

Let us first deal with the frequencies in  $E_1$ . Here we will take absolute values everywhere, which is fairly crude but conveys the major advantage that we will be able to easily eliminate the supremum in  $g_j$ . Note that since

$$|\hat{g}_{j'}(k)| \leq \|g_{j'}\|_X / \sqrt{N} \leq 2^{j'+2} / \sqrt{N}$$

we see that this case is vacuous unless

$$\frac{2^{j'+2}}{\sqrt{N}} \geq \frac{C_0 2^j}{c_{j,j'} \sqrt{N}}$$

or in other words

$$2^{j'-j} \geq \frac{C_0}{4c_{j,j'}}. \quad (7.9)$$

We then use the crude bound

$$|\hat{g}_j(k)| \leq \|g_j\|_X / \sqrt{N} \leq 2^{j+2} / \sqrt{N}$$

and the triangle inequality to conclude

$$\sup_{g_j \in A_j - A_{j+1}} Q_1(g_j, g_{j'}) \leq \frac{2^{j+2}}{\sqrt{N}} \sum_{k \in E_1} (I_k + \tau) |\hat{g}_{j'}(k)|.$$

By definition of  $E_1$ , we have

$$\begin{aligned} \sum_{k \in E_1} 2\tau |\hat{g}_{j'}(k)| &\leq \frac{2c_{j,j'}\tau\sqrt{N}}{C_0 2^j} \sum_{k \in \mathbf{Z}_N} |\hat{g}_{j'}(k)|^2 \\ &= \frac{2c_{j,j'}\tau\sqrt{N}}{C_0 2^j} \|g_{j'}\|_{\ell_2}^2 \\ &\leq \frac{Cc_{j,j'}\tau\sqrt{N}}{C_0 2^j}. \end{aligned}$$

Writing  $I_k + \tau = (I_k - \tau) + 2\tau$ , we conclude that

$$\sup_{g_j \in A_j - A_{j+1}} Q_1(g_j, g_{j'}) \leq \frac{2^{j+2}}{\sqrt{N}} \sum_{k \in E_1} (I_k - \tau) |\hat{g}_{j'}(k)| + \frac{Cc_{j,j'}\tau}{C_0}$$

and hence to prove (7.8) when  $i = 1$  it would suffice (if  $C_0$  is chosen sufficiently large) to show that

$$\mathbf{P} \left( \frac{2^{j+2}}{\sqrt{N}} \sum_{k \in E_1} (I_k - \tau) |\hat{g}_{j'}(k)| > c_{j,j'} \cdot \tau \right) = O(\exp(-\frac{C}{1+2^{2j'}} \cdot m \log^2 N)).$$

It thus suffices to show

$$\mathbf{P} \left( \left| \sum_{k \in E_1} (I_k - \tau) a(k) \right| \geq \gamma \right) = O(\exp(-\frac{C}{1+2^{2j'}} \cdot m \log^2 N))$$

where  $a(k) := |\hat{g}_{j'}(k)|$  and  $\gamma := \frac{c_{j,j'}\tau\sqrt{N}}{C_0 2^j}$ . Recall that

$$\|a(k)\|_{\ell_\infty(E_1)} = O(\|g_{j'}\|_X / \sqrt{N}) = O(2^{j'} / \sqrt{N})$$

and

$$\|a(k)\|_{\ell_2(E_1)} \leq \|\hat{g}_{j'}\|_{\ell_2} = \|g_{j'}\|_{\ell_2} = O(1).$$

We apply Lemma 6.6 and obtain

$$\mathbf{P} \left( \left| \sum_{k \in E_1} (I_k - \tau) a(k) \right| \geq \gamma \right) = O\left(\exp\left(-\frac{C\gamma^2}{4\tau + \gamma 2^{j'}/\sqrt{N}}\right)\right).$$

Using (7.9), we see that  $\gamma 2^{j'}/\sqrt{N} \geq c \cdot \tau$  for some absolute constant  $c > 0$ , and conclude that

$$\mathbf{P} \left( \left| \sum_{k \in E_1} (I_k - \tau) a(k) \right| \geq \gamma \right) = O\left(\exp\left(-\frac{C \cdot c_{j,j'} \cdot \tau N}{2^{j+j'}}\right)\right).$$

Taking logarithms, we deduce that this contribution will be acceptable if

$$\frac{1}{1 + 2^{2j'}} \cdot m \log^2 N \leq C \cdot \frac{c_{j,j'} \cdot \tau N}{2^{j+j'}}$$

which holds if

$$m \leq C \cdot \frac{c_{j,j'} \cdot \tau N}{\log^2 N}. \quad (7.10)$$

Consider now the  $i = 2$  case of (7.8). In this case we use (7.5) and the union bound, and reduce to showing that

$$\mathbf{P} (Q_2(g_j, g_{j'}) > c_{j,j'} \cdot \tau) = O\left(\exp\left(-\frac{C}{1 + 2^{2j}} m \log^2 N\right)\right) \quad (7.11)$$

for any  $g_j \in A_j - A_{j+1}$ .

Fix  $g_j$ , and set  $a(k) := \text{Re}(\hat{g}_j(k) \overline{\hat{g}_{j'}(k)})$ ; thus

$$Q_2(g_j, g_{j'}) = \sum_{k \in E_2} (I_k - \tau) a(k).$$

By definition of  $E_2$ , we have

$$\|a(k)\|_{\ell_\infty(E_2)} \leq O\left(\frac{2^j}{c_{j,j'} \sqrt{N}} \frac{\|g_j\|_X}{\sqrt{N}}\right) = O\left(\frac{2^{2j}}{c_{j,j'} N}\right)$$

while from Hölder and Plancherel

$$\|a(k)\|_{\ell_2(E_2)} \leq \|\hat{g}_{j'}\|_{\ell_2} \|\hat{g}_j\|_{\ell_\infty} = \frac{\|g_{j'}\|_{\ell_2} \|g_j\|_X}{\sqrt{N}} = O\left(\frac{2^j}{\sqrt{N}}\right).$$

We can apply Lemma 6.6 to conclude

$$\begin{aligned} \mathbf{P} (Q_2(g_j, g_{j'}) > c_{j,j'} \cdot \tau) &= O\left(\exp\left(-\frac{C \cdot c_{j,j'}^2 \cdot \tau^2}{\tau[2^{2j}/N] + \tau[c_{j,j'} 2^{2j}/c_{j,j'} N]}\right)\right) \\ &= O\left(\exp\left(-\frac{C \cdot c_{j,j'}^2 \cdot \tau N}{2^{2j}}\right)\right). \end{aligned}$$

Taking logarithms, we thus see that this contribution will be acceptable if

$$\frac{1}{1 + 2^{2j}} \cdot m \log^2 N \leq C \cdot \frac{c_{j,j'}^2 \cdot \tau N}{2^{2j}}$$

which holds if

$$m \leq C \cdot \frac{c_{j,j'}^2 \cdot \tau N}{\log^2 N}. \quad (7.12)$$

Since there are  $O(\log^2 N)$  pairs  $j, j'$ , we may select  $c_{j,j'} = c_0/\log^2 N$ , where  $c_0$  is small enough so that (7.7) holds. With this choice, the bound (7.3) follows provided that  $m \leq \alpha \cdot \tau N/\log^6 N$ . This concludes the proof of Lemma 4.3 (assuming Proposition 7.2). ■

## 7.1 Proof of entropy estimate

It remains to prove Proposition 7.2, to which we now turn. The material here is to a large extent borrowed from that in [4], [5], [34].

The entropy of the unit ball of a Hilbert space can be estimated using the *dual Sudakov inequality* of Pajor and Tomczak-Jaegerman [35] (See [6], [34] for a short “volume packing” proof, and [34] for further discussion):

**Lemma 7.3** [35] *Let  $H$  be a  $n$ -dimensional Hilbert space with norm  $\|\cdot\|_H$ , and let  $B_H$  be the associated unit ball. Let  $e_1, \dots, e_n$  be an orthonormal basis of the Hilbert space  $H$ , and let  $Z_1, \dots, Z_n \sim N(0, 1)$  be i.i.d. standard Gaussian random variables. Let  $\|\cdot\|_X$  be any other norm on  $\mathbf{C}^n$ . Then we have*

$$\mathcal{E}(B_H, B_X, r) \leq Cr^{-2} \cdot \mathbf{E}(\|\sum_{j=1}^n Z_j e_j\|_X)^2$$

where  $C$  is an absolute constant (independent of  $n$ ).

To apply this Lemma, we need to estimate the  $X$  norm of certain randomized signs. Fortunately, this is easily accomplished:

**Lemma 7.4** *Let  $f \in \ell_2(\mathbb{Z}_N)$  and  $Z(t)$ ,  $t \in \mathbb{Z}_N$ , be i.i.d. standard Gaussian random variables. Then*

$$\mathbf{E}(\|Zf\|_X) \leq C \cdot \sqrt{\log N} \cdot \|f\|_{\ell_2}.$$

*The same statement holds if the  $Z$ 's are i.i.d. Bernoulli symmetric random variables ( $Z(t) = \pm 1$  with equal probability).*

**Proof** Let us normalize  $\|f\|_{\ell_2} = 1$ . For any  $\lambda > 0$ , we have

$$\begin{aligned} \mathbf{P}(\|Zf\|_X > \lambda) &= \mathbf{P}\left(\left|\sum_{t \in \mathbb{Z}_N} Z(t)f(t)e^{-2\pi itk/N}\right| > \lambda \text{ for some } k \in \mathbb{Z}_N\right) \\ &\leq N \sup_{k \in \mathbb{Z}_N} \mathbf{P}\left(\left|\sum_{t \in \mathbb{Z}_N} Z(t)f(t)e^{-2\pi itk/N}\right| > \lambda\right). \end{aligned}$$

If the  $Z(t)$  are i.i.d. normalized Gaussians, then for each fixed  $k$ ,  $\sum_{t \in \mathbb{Z}_N} Z(t)f(t)e^{-2\pi itk/N}$  is a Gaussian with mean zero and standard deviation  $\|f\|_{\ell_2} = 1$ . Hence

$$\mathbf{P}(\|Zf\|_X > \lambda) \leq C \cdot N \cdot e^{-\lambda^2/2}.$$

Combining this with the trivial bound  $\mathbf{P}(\|Zf\|_X > \lambda) \leq 1$  and then integrating in  $\lambda$  gives the result. The claim for i.i.d. Bernoulli variables is similar but uses Hoeffding's inequality; we omit the standard details.  $\blacksquare$

Combining this lemma with Lemma 7.3, we immediately obtain

**Corollary 7.5** *Let  $E$  be a non-empty subset of  $\ell_2(\mathbb{Z}_N)$ ; note that  $\ell_2(E)$  is both a Hilbert space (with the usual Hilbert space structure), as well as a normed vector space with the  $X$  norm. For all  $r > 0$ , we have*

$$\mathcal{E}(B_{\ell_2(E)}, B_X, r) \leq Cr^{-2} \cdot |E| \cdot \log N.$$

Now we turn to the set  $U_m$  introduced in the preceding section. Since the number of sets  $E$  of cardinality  $m$  is  $\binom{N}{m} \leq N^m$ , we have the crude bound

$$N(U_m, B_X, r) \leq N^m \sup_{E \subseteq \mathbb{Z}_N, |E|=m} N(\mathcal{E}, B_X, r)$$

and hence by Corollary 7.5

$$\mathcal{E}(U_m, B_X, r) \leq C(1 + r^{-2}) m \log N. \quad (7.13)$$

This already establishes (7.4) in the range  $C^{-1} \leq r \leq C\sqrt{\log N}$ . However, this bound is quite poor when  $r$  is large. For instance, when  $r \geq m^{1/2}$  we have

$$\mathcal{E}(U_m, B_X, r) = 0 \quad (7.14)$$

since we have  $\|f\|_X < m^{1/2}$  whenever  $\|f\|_{\ell_2} \leq 1$  and  $|\text{supp}(f)| \leq m$ . In the regime  $1 \ll r \leq m^{1/2}$  we can use the following support reduction trick of Bourgain to obtain a better bound:

**Lemma 7.6** [4] *If  $r \geq C\sqrt{\log N}$  and  $m \geq C$ , then*

$$N(U_m, B_X, r) \leq N(U_{m/2+C\sqrt{m}}, B_X, \frac{r}{\sqrt{2} + C/\sqrt{m}} - C\sqrt{\log N}).$$

**Proof** Let  $f \in U_m$  and  $E := \text{supp}(f)$ , thus  $\|f\|_{\ell_2} \leq 1$  and  $|E| \leq m$ . Let  $\sigma(t) = \pm 1$  be i.i.d. Bernoulli symmetric variables. We write  $f = \sigma f + (1 - \sigma)f$ . From Lemma 7.4 for Bernoulli variables we have

$$\mathbf{E}(\|\sigma f\|_X) \leq C\sqrt{\log N}$$

and hence by Markov's inequality

$$\mathbf{P}(\|\sigma f\|_X \geq C\sqrt{\log N}) \leq \frac{1}{10}$$

for a suitable absolute constant  $C$ . Also observe that

$$\|(1 - \sigma)f\|_{\ell_2}^2 = \sum_{t \in E; \sigma(t) = -1} 4|f(t)|^2 = 2\|f\|_{\ell_2}^2 - 2 \sum_{t \in E} \sigma(t)|f(t)|^2,$$

and hence by Hoeffding's or Khintchine's inequalities and the normalization  $\|f\|_{\ell_2} \leq 1$

$$\mathbf{P}(\|(1 - \sigma)f\|_{\ell_2} \geq \sqrt{2} + C/\sqrt{m}) \leq \frac{1}{10}$$

for a suitable absolute constant  $C$ . In a similar spirit, we have

$$\text{supp}((1 - \sigma)f) = |\{t \in \text{supp}(f) : \sigma(t) = -1\}| = \frac{1}{2}\text{supp}(f) - \frac{1}{2}\sum_{t \in E} \sigma(t),$$

and hence

$$\mathbf{P}(\text{supp}((1 - \sigma)f) \geq \frac{m}{2} + C\sqrt{m}) \leq \frac{1}{10}$$

for a suitable absolute constant  $C$ . Combining all these estimates together, we see that there exists a deterministic choice of signs  $\sigma(t) = \pm 1$  (depending on  $f$  and  $E$ ) such that

$$\|\sigma f\|_X \leq C\sqrt{\log N}; \|(1 - \sigma)f\|_{\ell_2} \leq \sqrt{2} + C/\sqrt{m}; \text{supp}((1 - \sigma)f) \leq \frac{m}{2} + C\sqrt{m}.$$

In particular,  $f$  is within  $C\sqrt{\log N}$  (in  $X$  norm) from  $(\sqrt{2} + C/\sqrt{m}) \cdot U_{m/2+C\sqrt{m}}$ . We thus have

$$N(U_m, B_X, r) \leq N((\sqrt{2} + C/\sqrt{m})U_{m/2+C\sqrt{m}}, B_X, r - C\sqrt{\log N})$$

and the claim follows.  $\blacksquare$

Iterating this lemma roughly  $\log_{\sqrt{2}} \frac{r}{\sqrt{\log N}}$  times to reduce  $m$  and  $r$ , and then applying (7.13) once  $r$  becomes comparable with  $\sqrt{\log N}$ , we obtain

$$\mathcal{E}(U_m, B_X, r) \leq Cr^{-2} m (\log N)^2 \text{ whenever } C\sqrt{\log N} \leq r \leq m^{1/2},$$

which (together with (7.14)) yields (7.4) for all  $r \geq C\sqrt{\log N}$ .

It remains to address the case of small  $r$ , say  $N^{-2} < r < 1/2$ . A simple covering argument (see [34, Lemma 2.7]; the basic point is that  $B_{\ell_2(E)}$  can be covered by  $O(r^{-C|E|})$  translates of  $r \cdot B_{\ell_2}(E)$ ) gives the general inequality

$$\mathcal{E}(B_{\ell_2(E)}, B_X, r) \leq C|E| \log \frac{1}{r} + \mathcal{E}(B_{\ell_2(E)}, B_X, 1)$$

for  $0 < r < 1/2$ , and hence by Corollary 7.5

$$\mathcal{E}(B_{\ell_2(E)}, B_X, r) \leq C|E| \log \frac{1}{r} + C|E| \log N.$$

Arguing as in the proof of (7.13) we thus have

$$\mathcal{E}(U_m, B_X, r) \leq Cm(\log N + \log \frac{1}{r}),$$

which gives (7.4) in the range  $N^{-2} < r < 1/2$ . This completes the proof of Proposition 7.2.  $\blacksquare$

**Remark** The above argument did not use any algebraic properties of the Fourier transform other than the Plancherel identity and the pointwise bounds on the Fourier matrix by  $O(1/\sqrt{N})$ . Indeed all the results for the Fourier ensemble in this paper would also hold if the Fourier basis were replaced by another bounded orthogonal system. See [4] and [10] for further discussion of this issue.

## 8 ‘Universal’ Encoding

Our results interact significantly with the agenda of coding theory. In fact, one can think of the process of taking random measurements as some kind of universal coding strategy that we explain below. In a nutshell, consider an encoder/decoder pair which would operate roughly as follows:

- The Encoder and the Decoder share a collection  $O(K \log N)$  of random vectors ( $X_k$ ) where the  $X_k$ 's are independent Gaussian vectors with standard normal entries. In practice, we can imagine that the encoder would send the seed of a random generator so that the decoder would be able to reconstruct those ‘pseudo-random’ vectors.
- *Encoder.* To encode a discrete signal  $f$ , the encoder simply calculates the coefficients  $y_k = \langle f, X_k \rangle$  and quantizes the vector  $y$ .
- *Decoder.* The decoder then receives the quantized values and reconstructs a signal by solving the linear program (1.11).

This encoding/decoding scheme is of course very different from those commonly discussed in the literature of information theory. In this scheme, the encoder would not try to know anything about the signal, nor would exploit any special structure of the signal; it would blindly correlate the signal with noise and quantize the output—effectively doing very little work. In other words, the encoder would treat each signal in exactly the same way, hence the name “universal encoding.” There are several aspects of such a strategy which seem worth exploring:

- *Robustness.* A fundamental problem with most existing coding strategies is their fragility vis a vis bit-loss. Take JPEG 2000, the current digital still-picture compression standard, for example. All the bits in JPEG 2000 do not have the same value and if important bits are missing (e.g. because of packet loss), then there is simply no way the information can be retrieved accurately.

The situation is very different when one is using the scheme suggested above. Suppose for example that with  $O(K \log N)$  coefficients one achieves the distortion obeying the power-law

$$\|f - f^\sharp\|^2 \lesssim 1/K. \quad (8.1)$$

(This would correspond to the situation where our objects are bounded in  $\ell_1$ .) Thus receiving  $O(K \log N)$  random coefficients essentially allows to reconstruct a signal as precisely as if one knew the  $K$  largest coefficients.

Now suppose that in each packet of information, we have both encoded the (quantized) value of the coefficients  $y_k$  but also the label of the corresponding coefficients  $k$ . Consider now a situation in which half of the information is lost in the sense that only half of the coefficients are actually received. What is the accuracy of the decoded message  $f_{50\%}^\sharp$ ? This essentially corresponds to reducing the number  $K$  of randomly sampled coefficients by a factor of two, and so by (8.1) we see that the distortion would obey

$$\|f - f_{50\%}^\sharp\|^2 \lesssim 2/K \quad (8.2)$$

and, therefore, losses would turn to have *minimalistic* effects.

- *Security.* Suppose that someone would intercept the message. Then he/she would not be able to decode the message because he/she would not know in which random basis the coefficients are expressed. (In practice, in the case where one would exchange the seed of a random generator, one could imagine protecting it with standard technologies such as RSA. Thus this scheme can be viewed as a variant of the standard stream cipher, based on applying a XOR operation between the plain text and a pseudorandom keystream, but with the advantage of robustness.)
- *Cost Efficiency.* Nearly all coding scenarios work roughly as follows: we acquire a large number of measurements about an object of interest, which we then encode. This encoding process effectively discards most of the measured data so that only a fraction of the measurement is being transmitted. For concreteness, consider JPEG 2000, a prototype of a transform coder. We acquire a large number  $N$  of sample values of a digital image  $f$ . The encoder then computes all the  $N$  wavelet coefficients of  $f$ , and quantizes only the  $B \ll N$  largest, say. Hence only a very small fraction of the wavelet coefficients of  $f$  are actually transmitted.

In stark contrast, our encoder makes measurements that are immediately used. Suppose we could design sensors which could actually measure the correlations  $\langle f, X_k \rangle$ . Then not only the decoded object would be nearly as good (in the  $\ell_2$ -distance) as that obtained by knowing all the wavelet coefficients and selecting the largest (it is expected that the  $\ell_1$ -reconstruction is well-behaved vis a vis quantization), but we would effectively encode all the measured coefficients and thus, we would not discard any data available about  $f$  (except for the quantization).

There are, of course, other properties/questions of interest. Concerning the efficiency of this strategy for example, the discussion section will argue that this scheme also enjoys near optimal information theoretic properties in the sense that it would not use, asymptotically speaking, many more bits than the necessary minimum. This paper is not about the development of all of these properties, however, as this will be the object of separate publications. Rather, our intention here is merely to suggest the relevance of our work to other disciplines and explain how our results might provide a renewed perspective on some fundamental problems in information theory.

## 9 Discussion

### 9.1 Optimality

A natural question is whether the number of random samples we identified in this paper is, in some sense, optimal. Or would it be possible to obtain similar accuracies with far fewer observations? To make things concrete, suppose we are interested in the recovery of objects with bounded  $\ell_1$ -norm, e.g. the  $\ell_1$ -ball

$$B_1 := \{f : \|f\|_{\ell_1} \leq 1\}.$$

Theorem 1.4 states that by taking  $O(K \log N)$ , one achieves the reconstruction error

$$\|f - f^\#\|_{\ell_2} \leq 1/\sqrt{K},$$

with overwhelming probability. The question is then straightforward: is there a linear measurement process which would guarantee an accuracy of  $1/\sqrt{K}$  with far fewer measurements?

We believe that the answer to this question is negative, at least in the interesting range of errors where  $K \ll N$ , e.g.  $K \asymp N^\beta$ ,  $\beta < 1$ , and we now present some evidence supporting this conjecture.

The first piece of evidence is provided by estimates about the entropy of the  $\ell_1$ -ball. As in Definition 7.1 and for a given set  $\mathcal{F} \subset \mathbf{R}^N$ , we let  $N(\mathcal{F}, r)$  be the smallest number of Euclidean balls of radius  $r$  which cover  $\mathcal{F}$ . Equipped with this definition, we introduce the *entropy numbers*

$$e_k = \inf\{r > 0 : N(\mathcal{F}, r) \leq 2^{k-1}\}. \quad (9.1)$$

It is well-known that this definition has a natural interpretation in coding theory. Indeed, this says that to encode a signal from  $\mathcal{F}$  to within precision  $e_k$ , one would need at least  $k$  bits. (In fact, Kolmogorov introduced 'his entropy' as an alternative to Shannon's rate distortion function and proposed a notion of data compression for classes of signals as opposed to stochastic processes.) The point is that we know the entropy numbers for the  $\ell_1$ -ball up to a multiplicative constant [40, 30]

$$e_k \asymp \left( \frac{\log(N/k + 1)}{k} \right)^{1/2}, \quad \log N \leq k \leq N. \quad (9.2)$$

This says that if we would like to know an object  $f$  in the  $\ell_1$ -ball to within precision  $1/\sqrt{K}$  one would need to spend at least  $O(K \log(N/K))$  bits. That is, for  $K \asymp N^\beta$ ,  $\beta < 1$ , we would need to spend at least  $O(K \log N)$  bits.

Of course, entropy calculations would not exactly give lower bounds on our recovery problem because they assume finite precision (in some sense each coefficient only represents one bit of information although this may be 'a nonlinear bit') whereas we assumed infinite precision about the measurements  $y = F_\Omega f$ . To develop an insight about the intrinsic difficulty of our problem, consider the following geometric picture. Suppose we take  $k$  measurements  $F_\Omega f$ ; this sets the constraint that  $f$  live on an affine space  $f_0 + S$  where  $S$  is a linear subspace of co-dimension less or equal to  $k$ . Now *the data available for the problem cannot distinguish any object belonging to that plane*. Assume  $f$  is known to belong to the  $\ell_1$ -ball  $B_1$ , say, then the data cannot distinguish between any two points in the intersection  $B_1 \cap f_0 + S$ . Therefore, any reconstruction procedure  $f^*(y)$  based upon  $y = F_\Omega f$  would obey

$$\sup_{f \in \mathcal{F}} \|f - f^*\| \geq \frac{\text{diam}(B_1 \cap S)}{2}. \quad (9.3)$$

(When we take the supremum over all  $f$ , we may just assume that  $f$  be orthogonal to the measurements ( $y = 0$ ) since the diameter will of course be maximal in that case.) The goal is then to find  $S$  such that the above diameter be minimal. This connects with the agenda of approximation theory where this problem is known as finding the Gelfand  $n$ -width of the class  $B_1$  [36], as we explain below.

The *Gelfand* numbers of a set  $\mathcal{F}$  are defined as

$$c_k = \inf_S \left\{ \sup_{f \in \mathcal{F}} \|P_S f\| : \text{codim}(S) < k \right\}, \quad (9.4)$$

where  $P_S$  is, of course, the orthonormal projection on the subspace  $S$ . Now classical results [36] show that

$$c_k \geq c \cdot 1/\sqrt{k}$$

and, therefore, one would need to observe at least  $O(K)$  coefficients to achieve an accuracy less or equal to  $1/\sqrt{K}$ . Finer estimates are actually possible. A result of Carl [12, 37] shows that the Gelfand numbers dominate in a certain sense the entropy numbers. For example, the following relation holds,

$$\sup_{k \leq n} k^\alpha e_k \leq \rho_\alpha \cdot \sup_{k \leq n} k^\alpha c_k \quad \text{for all } n \geq 1,$$

for some universal constant  $\rho_\alpha$ . We apply this inequality with  $\alpha = 1/2$  together with (9.2) and obtain

$$\rho_{1/2} \cdot \sup_{k \leq n} k^{1/2} c_k \geq \sup_{k \leq n} k^{1/2} e_k \geq c \cdot \sup_{k \leq n} (\log(N/k + 1))^{1/2} = \sqrt{\log(N + 1)}.$$

In other words, for some values  $k^*$  of  $k$  we have

$$c_{k^*} \geq c \cdot \left( \frac{\log N}{k^*} \right)^{1/2}.$$

In short, we would need at least  $O(K \log N)$  measurements to know  $f$  within precision  $1/\sqrt{K}$ —at least for some values of  $K$ . Therefore, there is a range of accuracies over which our results seem provably optimal.

The above analysis extends to  $\ell_p$ -balls for  $p < 1$  which are smaller sets than those we considered in this paper

$$B_p := \{f : \|f\|_{\ell_p} \leq 1\} \subset w\ell_p(1),$$

and hence easier to recover (i.e. the worst case error for signal obeying (1.9) would be lower bounded by that of signals in  $B_p$ ). Now for  $\ell_p$ -balls,  $p \leq 1$  we have

$$e_k \asymp \left( \frac{\log(N/k + 1)}{k} \right)^{1/p-1/2}, \quad \log N \leq k \leq N. \quad (9.5)$$

Therefore, a similar argument shows that to obtain a reconstruction with worst-case error

$$\|f - f^*\| \leq K^{-r} \quad r = 1/p - 1/2,$$

one would need at least  $K \log N$  samples which is precisely the number of coefficients required in Theorem 1.4, possibly to within constant factors.

We emphasize that we merely hinted at optimality results. A careful argument would actually require (1) articulating the fact that the lower bounds would not change when we only ask for success with overwhelming probability and (2) possibly show that the optimality statement actually holds over a broad range of numbers of observed coefficients. We have partial results in this direction and hope to report on these in a forthcoming publication.

## 9.2 Robustness vis a vis Quantization

An important issue is to know whether our results are sensitive to perturbations or quantization errors. For example, suppose that the measurements  $y_k = \langle f, \psi_k \rangle$  are rounded up to the nearest multiple of  $q$ , say, so that the available information is of the form  $y_k^q$  with  $-q/2 \leq y_k^q - y_k \leq q/2$ . Then we would like to know whether the solution  $f^\#$  to (1.11) or better, of the variant

$$\min_g \|g\|_{\ell_1}, \quad \text{subject to} \quad \|F_\Omega g - y^q\|_{\ell_\infty} \leq q/2$$

still obeys error estimates such as those introduced in Theorem 1.4. Our analysis seems to be amenable to this situation and work in progress shows that there are ways of calibrating the quantization step  $q$  so that the quantization error introduced in the reconstruction would be small when compared to the main error term (1.16). Together with the entropy results of the last section, this would say that the Gaussian encoder/decoder pair discussed earlier would be information theoretically efficient.

## 9.3 Connections with other works

Our results are connected with very recent work of A. Gilbert, S. Muthukrishnan, and M. Strauss [26], [27]. In this work, one considers a discrete signal of length  $N$  which one would like to represent as a sparse superposition of sinusoids. In [26], the authors develop a randomized algorithm that essentially samples the signal  $f$  in the time domain  $O(B^2 \text{poly}(\log N))$  times ( $\text{poly}(\log N)$  denotes a polynomial term in  $\log N$ ) and returns a vector of approximate Fourier coefficients. They show that under certain conditions, this vector gives, with positive probability, an approximation to the discrete Fourier transform of  $\hat{f}$  which is almost as good as that obtained by keeping the  $B$ -largest entries of the discrete Fourier transform of  $\hat{f}$ . In [27], the algorithm was refined so that (1) only  $O(B \text{poly}(\log N))$  samples are needed and (2) so that the algorithm runs in  $O(B \text{poly}(\log N))$  time which truly is a remarkable feat. To achieve this gain, however, one has to sample the signal on highly structured random grids.

Our approach is different in several aspects. First and foremost, we are given a fixed set of nonadaptive measurements. In other words, the way in which we stated the problem does not give us the 'luxury' of adaptively sampling the signals as in [27]. In this context, it is unclear how the methodology presented in [26, 27] would allow reconstructing the signal  $f$  from  $O(B \text{poly}(\log N))$  arbitrary sampled values. In contrast, our results guarantee that an accurate reconstruction is possible for nearly all possible measurements sets taken from ensembles obeying **UUP** and **ERP**. Second, the methodology there essentially concerns the recovery of spiky signals from frequency samples and do not address other setups. Yet, there certainly is a similar flavor in the statements of their results. Of special interest is whether some of the ideas developed by this group of researchers might be fruitful to attack problems such as those discussed in this article.

Last but not least, while finishing the write-up of this paper, we became aware of very recent work by David Donoho on a similar project, [18, 19].

## References

- [1] Z. D. Bai and Y. Q. Yin, Limit of the smallest eigenvalue of a large-dimensional sample covariance matrix. *Ann. Probab.* **21** (1993), 1275–1294.
- [2] P. Bloomfield and W. Steiger, *Least Absolute Deviations: Theory, Applications, and Algorithms*. Birkhäuser, Boston, 1983.
- [3] S. Boucheron, G. Lugosi, and P. Massart, A sharp concentration inequality with applications, *Random Structures Algorithms* **16** (2000), 277–292.
- [4] J. Bourgain, Bounded orthogonal systems and the  $\Lambda(p)$ -set problem, *Acta Math.* **162** (1989), 227–245.
- [5] J. Bourgain, Remarks on Halasz-Montgomery type inequalities, Geometric aspects of functional analysis (Israel, 1992–1994), 25–39, *Oper. Theory Adv. Appl.*, **77**, Birkhäuser, Basel, 1995.
- [6] J. Bourgain, J. Lindenstrauss, V. Milman, Approximation of zonoids by zonotopes, *Acta Math.* **162** (1989), 73–141.
- [7] E. J. Candès, and P. S. Loh, Image reconstruction with ridgelets, SURF Technical report, California Institute of Technology, 2002.
- [8] E. J. Candès, D. L. Donoho, New Tight Frames of Curvelets and Optimal Representations of Objects with Piecewise  $C^2$  Singularities, *Comm. on Pure and Appl. Math.*, **57** (2004), 219–266.
- [9] E. J. Candès, J. Romberg, and T. Tao, Robust Uncertainty Principles: Exact Signal Reconstruction from Highly Incomplete Frequency Information, Technical Report, California Institute of Technology. *Submitted for publication*.
- [10] E. J. Candès, and J. Romberg, The Role of Sparsity and Incoherence for Exactly Reconstructing a Signal from Limited Measurements, Technical Report, California Institute of Technology.
- [11] E. J. Candès, and J. Romberg, Quantitative Robust Uncertainty Principles and Optimally Sparse Decompositions, Technical Report, California Institute of Technology.
- [12] B. Carl, Entropy numbers,  $s$ -numbers, and eigenvalue problems. *J. Funct. Anal.* **41** (1981), 290–306.
- [13] S. S. Chen, Basis Pursuit, Stanford Ph. D. Thesis, 1995.
- [14] S. S. Chen, D. L. Donoho, and M. A. Saunders, Atomic decomposition by basis pursuit, *SIAM J. Scientific Computing* **20** (1999), 33–61.
- [15] K. R. Davidson and S. J. Szarek, Local operator theory, random matrices and Banach spaces, In: *Handbook in Banach Spaces* Vol I, ed. W. B. Johnson, J. Lindenstrauss, Elsevier (2001), 317–366.
- [16] D. C. Dobson, and F. Santosa, Recovery of blocky images from noisy and blurred data, *SIAM J. Appl. Math.* **56** (1996), 1181–1198.

- [17] D. L. Donoho, M. Vetterli, R. A. DeVore, and I. Daubechies. Data compression and harmonic analysis, *IEEE Trans. Inform. Theory* **44** (1998), 2435–2476.
- [18] D. L. Donoho, For Most Large Underdetermined Systems of Linear Equations the Minimal  $\ell_1$ -norm Solution is also the Sparsest Solution, Manuscript, September 2004.
- [19] D. L. Donoho, Compressed Sensing, Manuscript, September 2004.
- [20] D.L. Donoho, P.B. Stark, Uncertainty principles and signal recovery, *SIAM J. Appl. Math.* **49** (1989), 906–931.
- [21] D.L. Donoho and X. Huo, Uncertainty principles and ideal atomic decomposition, *IEEE Transactions on Information Theory*, **47** (2001), 2845–2862.
- [22] D. L. Donoho and M. Elad, Optimally sparse representation in general (nonorthogonal) dictionaries via  $\ell_1$  minimization, *Proc. Natl. Acad. Sci. USA* **100** (2003), 2197–2202.
- [23] El Karoui, New Results about Random Covariance Matrices and Statistical Applications, Stanford Ph. .D. Thesis, August 2004.
- [24] H. G. Feichtinger, Atomic characterizations of modulation spaces through Gabor-type representations. *Rocky Mountain J. Math.* **19** (1989), 113–125.
- [25] J. J. Fuchs, On sparse representations in arbitrary redundant bases, *IEEE Transactions on Information Theory*, **50** (2004), 1341–1344.
- [26] A. C. Gilbert, S. Guha, P. Indyk, S. Muthukrishnan, M. Strauss, Near-optimal sparse Fourier representations via sampling, *34th ACM Symposium on Theory of Computing*, Montréal, May 2002.
- [27] A. C. Gilbert, S. Muthukrishnan, and M. Strauss, Beating the  $B^2$  bottleneck in estimating  $B$ -term Fourier representations, unpublished manuscript, May 2004.
- [28] R. Gribonval and M. Nielsen, Sparse representations in unions of bases. *IEEE Trans. Inform. Theory* **49** (2003), 3320–3325.
- [29] I. M. Johnstone, On the distribution of the largest eigenvalue in principal components analysis. *Ann. Statist.* **29** (2001), 295–327.
- [30] T. Kühn. A lower estimate for entropy numbers. *J. Approx. Theory* **110** (2001), 120–124.
- [31] Ledoux, M, *The concentration of measure phenomenon*. Mathematical Surveys and Monographs **89**, . American Mathematical Society, Providence, RI, 2001.
- [32] A. E. Litvak, A. Pajor M. Rudelson, and N. Tomczak-Jaegermann, Smallest singular value of random matrices and geometry of random polytopes, manuscript, August 2004.
- [33] V. A. Marchenko and L. A. Pastur, Distribution of eigenvalues in certain sets of random matrices, *Mat. Sb. (N.S.)* **72** (1967), 407–535 (in Russian).
- [34] G. Mockenhaupt and W. Schlag, *On the Hardy-Littlewood problem for random sets*, preprint.

- [35] A. Pajor, N. Tomczak-Jaegermann, Subspaces of small codimension of finite-dimensional Banach spaces, *Proc. Amer. Math. Soc.* **97** (1986), 637–642.
- [36] A. Pinkus, *N-Widths in Approximation Theory*. Springer-Verlag, Berlin, 1985.
- [37] G. Pisier. *The Volume of Convex Bodies and Banach Space Geometry*. Cambridge Tracts in Mathematics **94**, Cambridge University Press, Cambridge, 1989.
- [38] L. I. Rudin, S. Osher, and E. Fatemi. Nonlinear total variation based noise removal algorithm, *Physica D* **60**, 259–268.
- [39] F. Santosa, and W. W. Symes, Linear inversion of band-limited reflection seismograms, *SIAM J. Sci. Statist. Comput.* **7** (1986), 1307–1330.
- [40] C. Schutt. Entropy numbers of diagonal operators between symmetric Banach spaces. *J. Approx. Theory* **40** (1984), 121–128.
- [41] J. W. Silverstein, The smallest eigenvalue of a large dimensional Wishart matrix, *Ann. Probab.* **13** (1985), 1364–1368.
- [42] S. J. Szarek, Condition numbers of random matrices, *J. Complexity* **7** (1991), 131–149.