Robust Uncertainty Principles: Exact Signal Reconstruction From Highly Incomplete Frequency Information

Emmanuel J. Candès, Justin Romberg, *Member, IEEE*, and Terence Tao

***Abstract*—This paper considers the model problem of reconstructing an object from incomplete frequency samples. Consider a discrete-time signal $f \in \boldsymbol{C}^N$ and a randomly chosen set of frequencies Ω. Is it possible to reconstruct f from the partial knowledge of its Fourier coefficients on the set Ω?**

A typical result of this paper is as follows. Suppose that f is a superposition of $|T|$ spikes $f(t) = \sum_{\tau \in T} f(\tau)\delta(t-\tau)$ obeying

$$|T| \leq C_M \cdot (\log N)^{-1} \cdot |\Omega|$$

for some constant $C_M > 0$. We do not know the locations of the spikes nor their amplitudes. Then with probability at least $1 - O(N^{-M})$, f can be reconstructed exactly as the solution to the ℓ_1 minimization problem

$$\min_g \sum_{t=0}^{N-1} |g(t)|, \quad \text{s.t. } \hat{g}(\omega) = \hat{f}(\omega) \text{ for all } \omega \in \Omega.$$

In short, exact recovery may be obtained by solving a convex optimization problem. We give numerical values for C_M which depend on the desired probability of success. Our result may be interpreted as a novel kind of nonlinear sampling theorem. In effect, it says that any signal made out of $|T|$ spikes may be recovered by convex programming from almost every set of frequencies of size $O(|T| \cdot \log N)$. Moreover, this is nearly optimal in the sense that *any* method succeeding with probability $1 - O(N^{-M})$ would in general require a number of frequency samples at least proportional to $|T| \cdot \log N$.

The methodology extends to a variety of other situations and higher dimensions. For example, we show how one can reconstruct a piecewise constant (one- or two-dimensional) object from incomplete frequency samples—provided that the number of jumps (discontinuities) obeys the condition above—by minimizing other convex functionals such as the total variation of f.

***Index Terms*—Convex optimization, duality in optimization, free probability, image reconstruction, linear programming, random matrices, sparsity, total-variation minimization, trigonometric expansions, uncertainty principle.**

Manuscript received June 10, 2004; revised September 9, 2005. the work of E. J. Candes is supported in part by the National Science Foundation under Grant DMS 01-40698 (FRG) and by an Alfred P. Sloan Fellowship. The work of J. Romberg is supported by the National Science Foundation under Grants DMS 01-40698 and ITR ACI-0204932. The work of T. Tao is supported in part by a grant from the Packard Foundation.

E. J. Candes and J. Romberg are with the Department of Applied and Computational Mathematics, California Institute of Technology, Pasadena, CA 91125 USA (e-mail: emmanuel@acm.caltech.edu, jrom@acm.caltech.edu).

T. Tao is with the Department of Mathematics, University of California, Los Angeles, CA 90095 USA (e-mail: tao@math.ucla.edu).

Communicated by A. Høst-Madsen, Associate Editor for Detection and Estimation.

Digital Object Identifier 10.1109/TIT.2005.862083

I. Introduction

In many applications of practical interest, we often wish to reconstruct an object (a discrete signal, a discrete image, etc.) from incomplete Fourier samples. In a discrete setting, we may pose the problem as follows; let $\hat{f}$ be the Fourier transform of a discrete object $f(t)$, $t = (t_1, \ldots, t_d) \in \mathbb{Z}_N^d := \{0, 1, \ldots, N-1\}^d$

$$\hat{f}(\omega) = \sum_{t \in \mathbb{Z}_N^d} f(t) e^{-2\pi i(\omega_1 t_1 + \cdots + \omega_d t_d)/N}.$$

The problem is then to recover f from partial frequency information, namely, from $\hat{f}(\omega)$, where $\omega = (\omega_1, \ldots, \omega_d)$ belongs to some set Ω of cardinality less than N^d—the size of the discrete object.

In this paper, we show that we can recover f *exactly* from observations $\hat{f}|_\Omega$ on small set of frequencies provided that f is *sparse*. The recovery consists of solving a straightforward optimization problem that finds $f^\sharp$ of minimal complexity with $\hat{f}^\sharp(\boldsymbol{\omega}) = \hat{f}(\boldsymbol{\omega}), \forall\, \boldsymbol{\omega} \in \Omega$.

A. A Puzzling Numerical Experiment

This idea is best motivated by an experiment with surprisingly positive results. Consider a simplified version of the classical tomography problem in medical imaging: we wish to reconstruct a two–dimensional image $f(t_1, t_2)$ from samples $\hat{f}|_\Omega$ of its discrete Fourier transform on a star-shaped domain Ω [1]. Our choice of domain is not contrived; many real imaging devices collect high-resolution samples along radial lines at relatively few angles. Fig. 1(b) illustrates a typical case where one gathers 512 samples along each of 22 radial lines.

Frequently discussed approaches in the literature of medical imaging for reconstructing an object from polar frequency samples are the so-called filtered backprojection algorithms. In a nutshell, one assumes that the Fourier coefficients at all of the unobserved frequencies are zero (thus reconstructing the image of "minimal energy" under the observation constraints). This strategy does not perform very well, and could hardly be used for medical diagnostics [2]. The reconstructed image, shown in Fig. 1(c), has severe nonlocal artifacts caused by the angular undersampling. A good reconstruction algorithm, it seems, would have to guess the values of the missing Fourier coefficients. In other words, one would need to interpolate $\hat{f}(\omega_1, \omega_2)$. This seems highly problematic, however; predictions of Fourier coefficients from their neighbors are very delicate, due to the global and highly oscillatory nature of the Fourier transform. Going

0018-9448/$20.00 © 2006 IEEE

Authorized licensed use limited to: IEEE Xplore. Downloaded on December 30, 2008 at 06:05 from IEEE Xplore. Restrictions apply.

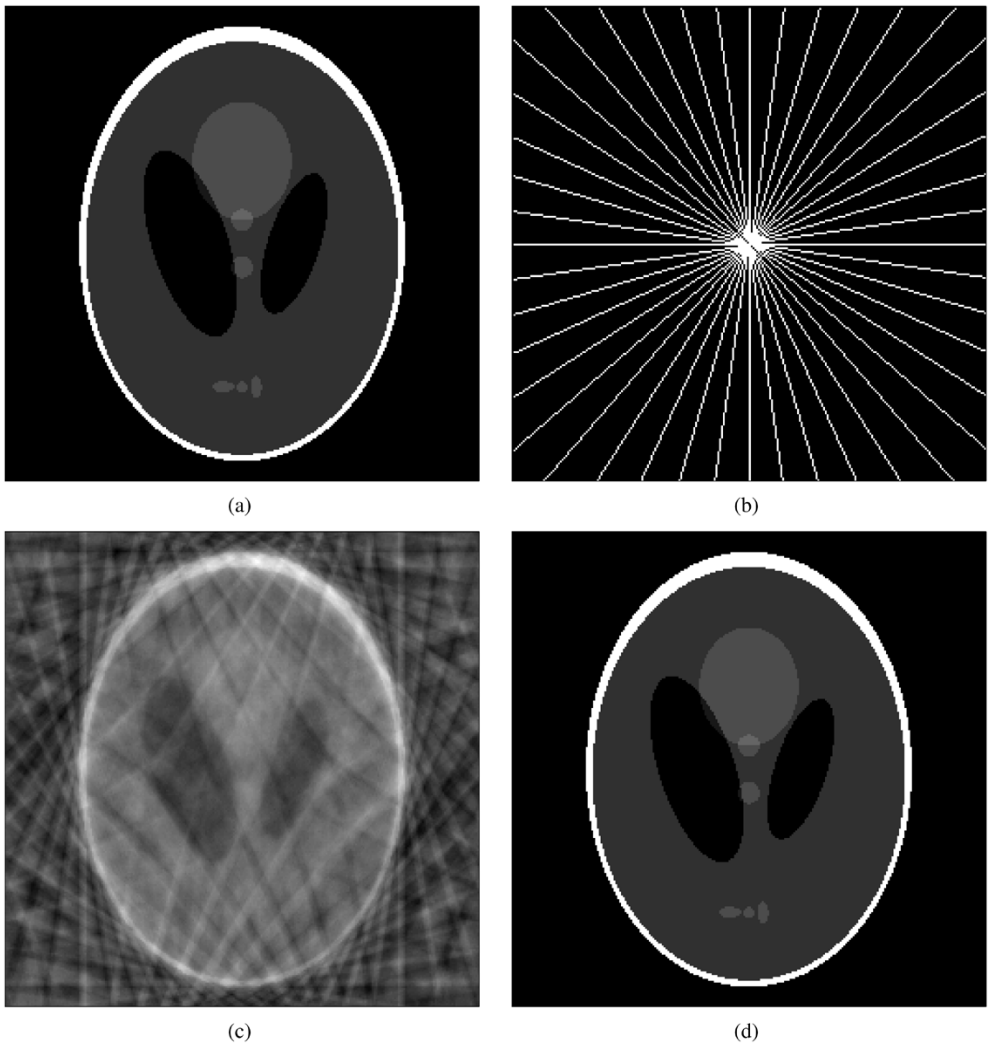

Fig. 1. Example of a simple recovery problem. (a) The Logan–Shepp phantom test image. (b) Sampling domain Ω in the frequency plane; Fourier coefficients are sampled along 22 approximately radial lines. (c) Minimum energy reconstruction obtained by setting unobserved Fourier coefficients to zero. (d) Reconstruction obtained by minimizing the total variation, as in (1.1). The reconstruction is an exact replica of the image in (a).

back to the example in Fig. 1, we can see the problem immediately. To recover frequency information near $(2\pi\omega_1/N, 2\pi\omega_2/N)$, where $2\pi\omega_1/N$ is near $\pm\pi$, we would need to interpolate $\hat{f}$ at the Nyquist rate $2\pi/N$. However, we only have samples at rate about $\pi/22$; the sampling rate is almost 50 times smaller than the Nyquist rate!

We propose instead a strategy based on convex optimization. Let $\|g\|_{TV}$ be the total-variation norm of a two-dimensional (2D) object g. For discrete data $g(t_1, t_2)$, $0 \le t_1, t_2 \le N-1$

$$\|g\|_{TV} = \sum_{t_1,t_2} \sqrt{|D_1 g(t_1,t_2)|^2 + |D_2 g(t_1,t_2)|^2}$$

where D_1 is the finite difference $D_1 g = g(t_1,t_2) - g(t_1-1,t_2)$ and $D_2 g = g(t_1,t_2) - g(t_1,t_2-1)$. To recover f from partial Fourier samples, we find a solution $f^\sharp$ to the optimization problem

$$\min \|g\|_{TV} \text{ subject to } \hat{g}(\boldsymbol{\omega}) = \hat{f}(\boldsymbol{\omega}) \text{ for all } \omega \in \Omega. \qquad (1.1)$$

In a nutshell, given partial observation $\hat{f}_{|\Omega}$, we seek a solution $f^\sharp$ with minimum complexity—called here the total variation (TV)—and whose "visible" coefficients match those of the unknown object f. Our hope here is to partially erase some of the artifacts that classical reconstruction methods exhibit (which tend to have large TV norm) while maintaining fidelity to the observed data via the constraints on the Fourier coefficients of the reconstruction. (Note that the TV norm is widely used in image processing, see [31] for example.)

When we use (1.1) for the recovery problem illustrated in Fig. 1 (with the popular Logan–Shepp phantom as a test image), the results are surprising. The reconstruction is *exact*; that is, $f^\sharp = f$! This numerical result is also not special to this phantom. In fact, we performed a series of experiments of this type and obtained perfect reconstruction on many similar test phantoms.

B. Main Results

This paper is about a quantitative understanding of this very special phenomenon. For which classes of signals/images can we expect perfect reconstruction? What are the tradeoffs between complexity and number of samples? In order to answer these questions, we first develop a fundamental mathematical understanding of a special 1D model problem. We then exhibit

Authorized licensed use limited to: IEEE Xplore. Downloaded on December 30, 2008 at 06:05 from IEEE Xplore. Restrictions apply.

reconstruction strategies which are shown to exactly reconstruct certain unknown signals, and can be extended for use in a variety of related and sophisticated reconstruction applications.

For a signal $f \in \boldsymbol{C}^N$, we define the classical discrete Fourier transform $\mathcal{F}f = \hat{f} : \boldsymbol{C}^N \to \boldsymbol{C}^N$ by

$$\hat{f}(\omega) := \sum_{t=0}^{N-1} f(t) e^{-2\pi i \omega t/N}, \qquad \omega = 0, 1, \ldots, N-1. \quad (1.2)$$

If we are given the value of the Fourier coefficients $\hat{f}(\omega)$ for *all* frequencies $\omega \in \mathbb{Z}_N$, then one can obviously reconstruct f exactly via the Fourier inversion formula

$$f(t) = \frac{1}{N} \sum_{\omega=0}^{N-1} \hat{f}(\omega) e^{2\pi i \omega t/N}.$$

Now suppose that we are only given the Fourier coefficients $\hat{f}|_\Omega$ sampled on some partial subset $\Omega \subsetneq \mathbb{Z}_N$ of all frequencies. Of course, this is not enough information to reconstruct f exactly in general; f has N degrees of freedom and we are only specifying $|\Omega| < N$ of those degrees (here and below $|\Omega|$ denotes the cardinality of Ω).

Suppose, however, that we also specify that f is supported on a small (but *a priori* unknown) subset T of $\mathbb{Z}_N$; that is, we assume that f can be written as a sparse superposition of spikes

$$f(t) = \sum_{\tau \in T} f(\tau) \delta(t - \tau), \qquad \delta(t) = 1_{\{t=0\}}.$$

In the case where N is prime, the following theorem tells us that it is possible to recover f exactly if $|T|$ is small enough.

Theorem 1.1: Suppose that the signal length N is a prime integer. Let Ω be a subset of $\{0, \ldots, N-1\}$, and let f be a vector supported on T such that

$$|T| \leq \frac{1}{2} |\Omega|. \quad (1.3)$$

Then f can be reconstructed uniquely from Ω and $\hat{f}|_\Omega$. Conversely, if Ω is not the set of all N frequencies, then there exist distinct vectors f, g such that $|\mathrm{supp}(f)|, |\mathrm{supp}(g)| \leq \frac{1}{2}|\Omega| + 1$ and such that $\hat{f}|_\Omega = \hat{g}|_\Omega$.

Proof: We will need the following lemma [3], from which we see that with knowledge of T, we can reconstruct f uniquely (using linear algebra) from $\hat{f}|_\Omega$.

Lemma 1.2: ([3, Corollary 1.4]) Let N be a prime integer and T, Ω be subsets of $\mathbb{Z}_N$. Put $\ell_2(T)$ (resp., $\ell_2(\Omega)$) to be the space of signals that are zero outside of T (resp., Ω). The restricted Fourier transform $\mathcal{F}_{T \to \Omega} : \ell_2(T) \to \ell_2(\Omega)$ is defined as

$$\mathcal{F}_{T \to \Omega} f := \hat{f}|_\Omega \text{ for all } f \in \ell_2(T).$$

If $|T| = |\Omega|$, then $\mathcal{F}_{T \to \Omega}$ is a bijection; as a consequence, we thus see that $\mathcal{F}_{T \to \Omega}$ is injective for $|T| \leq |\Omega|$ and surjective for $|T| \geq |\Omega|$. Clearly, the same claims hold if the Fourier transform $\mathcal{F}$ is replaced by the inverse Fourier transform $\mathcal{F}^{-1}$.

To prove Theorem 1.1, assume that $|T| \leq \frac{1}{2}|\Omega|$. Suppose for contradiction that there were two objects f, g such that $\hat{f}|_\Omega = \hat{g}|_\Omega$ and $|\mathrm{supp}(f)|, |\mathrm{supp}(g)| \leq \frac{1}{2}|\Omega|$. Then the Fourier transform of $f - g$ vanishes on Ω, and $|\mathrm{supp}(f - g)| \leq |\Omega|$. By Lemma 1.2, we see that $\mathcal{F}_{\mathrm{supp}(f-g) \to \Omega}$ is injective, and thus $f - g = 0$. The uniqueness claim follows.

We now examine the converse claim. Since $|\Omega| < N$, we can find disjoint subsets T, S of $\mathbb{Z}_N$ such that $|T|, |S| \leq \frac{1}{2}|\Omega| + 1$ and $|T| + |S| = |\Omega| + 1$. Let ω_0 be some frequency which does not lie in Ω. Applying Lemma 1.2, we have that $\mathcal{F}_{T \cup S \to \Omega \cup \{\omega_0\}}$ is a bijection, and thus we can find a vector h supported on $T \cup S$ whose Fourier transform vanishes on Ω but is nonzero on ω_0; in particular, h is not identically zero. The claim now follows by taking $f := h|_T$ and $g := -h|_S$. □

Note that if N is not prime, the lemma (and hence the theorem) fails, essentially because of the presence of nontrivial subgroups of $\mathbb{Z}_N$ with addition modulo N; see Sections I-C and -D for concrete counter examples, and [3], [4] for further discussion. However, it is plausible to think that Lemma 1.2 continues to hold for nonprime N if T and Ω are assumed to be *generic*—in particular, they are not subgroups of $\mathbb{Z}_N$, or cosets of subgroups. If T and Ω are selected uniformly at random, then it is expected that the theorem holds with probability very close to one; one can indeed presumably quantify this statement by adapting the arguments given above but we will not do so here. However, we refer the reader to Section I-G for a rapid presentation of informal arguments pointing in this direction.

A refinement of the argument in Theorem 1.1 shows that for fixed subsets T, S in the time domain and Ω in the frequency domain, the space of vectors f, g supported on T, S such that $\hat{f}|_\Omega = \hat{g}|_\Omega$ has dimension $|T \cup S| - |\Omega|$ when $|T \cup S| \geq |\Omega|$, and has dimension $|T \cap S|$ otherwise. In particular, if we let $\Sigma(N_t)$ denote those vectors whose support has size at most N_t, then the set of vectors in $\Sigma(N_t)$ which cannot be reconstructed uniquely in this class from the Fourier coefficients sampled at Ω, is contained in a finite union of linear spaces of dimension at most $2N_t - |\Omega|$. Since $\Sigma(N_t)$ itself is a finite union of linear spaces of dimension N_t, we thus see that recovery of f from $\hat{f}|_\Omega$ is in principle possible *generically* whenever $|\mathrm{supp}(f)| = N_t < |\Omega|$; once $N_t \geq |\Omega|$, however, it is clear from simple degrees-of-freedom arguments that unique recovery is no longer possible. While our methods do not quite attain this theoretical upper bound for correct recovery, our numerical experiements suggest that they do come within a constant factor of this bound (see Fig. 2).

Theorem 1.1 asserts that one can reconstruct f from $2|T|$ frequency samples (and that, in general, there is no hope to do so from fewer samples). In principle, we can recover f exactly by solving the combinatorial optimization problem

$$(P_0) \qquad \min_{g \in \boldsymbol{C}^N} \|g\|_{\ell_0}, \quad \hat{g}|_\Omega = \hat{f}|_\Omega, \quad (1.4)$$

where $\|g\|_{\ell_0}$ is the number of nonzero terms $\#\{t, g(t) \neq 0\}$. This is a combinatorial optimization problem, and solving (1.4) directly is infeasible even for modest-sized signals. To the best of our knowledge, one would essentially need to let T vary over all subsets $T \subset \{0, \ldots, N-1\}$ of cardinality $|T| \leq \frac{1}{2}|\Omega|$, checking for each one whether f is in the range of $\mathcal{F}_{T \to \Omega}$ or not, and then invert the relevant minor of the Fourier matrix to recover f once T is determined. Clearly, this is computationally

Authorized licensed use limited to: IEEE Xplore. Downloaded on December 30, 2008 at 06:05 from IEEE Xplore. Restrictions apply.

very expensive since there are exponentially many subsets to check; for instance, if $|\Omega| \sim N/2$, then the number of subsets scales like $4^N \cdot 3^{-3N/4}$! As an aside comment, note that it is also not clear how to make this algorithm robust, especially since the results in [3] do not provide any effective lower bound on the determinant of the minors of the Fourier matrix, see Section VI for a discussion of this point.

A more computationally efficient strategy for recovering f from Ω and $\hat{f}|_\Omega$ is to solve the convex problem

$$(P_1) \qquad \min_{g \in \boldsymbol{C}^N} \|g\|_{\ell_1} := \sum_{t \in \mathbb{Z}_N} |g(t)|, \quad \hat{g}|_\Omega = \hat{f}|_\Omega. \qquad (1.5)$$

The key result in this paper is that the solutions to (P_0) and (P_1) are *equivalent* for an overwhelming percentage of the choices for T and Ω with $|T| \leq \alpha \cdot |\Omega| / \log N$ ($\alpha > 0$ is a constant): in these cases, solving the convex problem (P_1) recovers f exactly.

To establish this upper bound, we will assume that the observed Fourier coefficients are *randomly sampled*. Given the number N_ω of samples to take in the Fourier domain, we choose the subset Ω uniformly at random from all sets of this size; i.e., each of the $\binom{N}{N_\omega}$ possible subsets are equally likely. Our main theorem can now be stated as follows.

Theorem 1.3: Let $f \in \boldsymbol{C}^N$ be a discrete signal supported on an unknown set T, and choose Ω of size $|\Omega| = N_\omega$ uniformly at random. For a given accuracy parameter M, if

$$|T| \leq C_M \cdot (\log N)^{-1} \cdot |\Omega| \qquad (1.6)$$

then with probability at least $1 - O(N^{-M})$, the minimizer to the problem (1.5) is unique and is equal to f.

Notice that (1.6) essentially says that $|T|$ is of size $|\Omega|$, modulo a constant and a logarithmic factor. Our proof gives an explicit value of C_M, namely, $C_M \asymp 1/[23(M+1)]$ (valid for $|\Omega| \leq N/4$, $M \geq 2$, and $N \geq 20$, say) although we have not pursued the question of exactly what the optimal value might be.

In Section V, we present numerical results which suggest that in practice, we can expect to recover *most* signals f more than 50% of the time if the size of the support obeys $|T| \leq |\Omega|/4$. By most signals, we mean that we empirically study the success rate for randomly selected signals, and do not search for the worst case signal f—that which needs the most frequency samples. For $|T| \leq |\Omega|/8$, the recovery rate is above 90%. Empirically, the constants $1/4$ and $1/8$ do not seem to vary for N in the range of a few hundred to a few thousand.

C. For Almost Every Ω

As the theorem allows, there exist sets Ω and functions f for which the ℓ_1-minimization procedure does not recover f correctly, even if $|\mathrm{supp}(f)|$ is much smaller than $|\Omega|$. We sketch two counter examples.

- *A discrete Dirac comb*. Suppose that N is a perfect square and consider the picket-fence signal which consists of spikes of unit height and with uniform spacing equal to $\sqrt{N}$. This signal is often used as an extremal point for uncertainty principles [4], [5] as one of its remarkable properties is its invariance through the Fourier transform. Hence, suppose that Ω is the set of all frequencies but the multiples of $\sqrt{N}$, namely, $|\Omega| = N - \sqrt{N}$. Then $\hat{f}|_\Omega = 0$ and obviously the reconstruction is identically zero.
  Note that the problem here does not really have anything to do with ℓ_1-minimization per se; f cannot be reconstructed from its Fourier samples on Ω thereby showing that Theorem 1.1 does not work "as is" for arbitrary sample sizes.
- *Boxcar signals.* The example above suggests that in some sense $|T|$ must not be greater than about $\sqrt{|\Omega|}$. In fact, there exist more extreme examples. Assume the sample size N is large and consider, for example, the indicator function f of the interval

  $$T := \{t : -N^{-0.01} < t - N/2 < N^{0.01}\}$$

  and let Ω be the set $\Omega := \{\omega : N/3 < \omega < 2N/3\}$. Let h be a function whose Fourier transform $\hat{h}$ is a nonnegative bump function adapted to the interval $\{\omega : -N/6 < \omega < N/6\}$ which equals 1 when $-N/12 < \omega < N/12$. Then $|h(t)|^2$ has Fourier transform vanishing in Ω, and is rapidly decreasing away from $t = 0$; in particular, we have $|h(t)|^2 = O(N^{-100})$ for $t \notin T$. On the other hand, one easily computes that $|h(0)|^2 > c$ for some absolute constant $c > 0$. Because of this, the signal $f - \varepsilon|h|^2$ will have smaller ℓ_1-norm than f for $\varepsilon > 0$ sufficiently small (and N sufficiently large), while still having the same Fourier coefficients as f on Ω. Thus, in this case f is not the minimizer to the problem (P_1), despite the fact that the support of f is much smaller than that of Ω.

The above counter examples relied heavily on the special choice of Ω (and to a lesser extent of $\mathrm{supp}(f)$); in particular, it needed the fact that the complement of Ω contained a large interval (or more generally, a long arithmetic progression). But for most sets Ω, large arithmetic progressions in the complement do not exist, and the problem largely disappears. In short, Theorem 1.3 essentially says that for *most* sets of T of size about $|\Omega|$, there is no loss of information.

D. Optimality

Theorem 1.3 states that for any signal f supported on an arbitrary set T in the time domain, (P_1) recovers f exactly—with high probability— from a number of frequency samples that is within a constant of $M \cdot |T| \log N$. It is natural to wonder whether this is a fundamental limit. In other words, is there an algorithm that can recover an arbitrary signal from far fewer random observations, and with the same probability of success?

It is clear that the number of samples needs to be at least proportional to $|T|$, otherwise, $\mathcal{F}_{T \to \Omega}$ will not be injective. We argue here that it must also be proportional to $M \log N$ to guarantee recovery of certain signals from the vast majority of sets Ω of a certain size.

Suppose f is the Dirac comb signal discussed in the previous section. If we want to have a chance of recovering f, then at the very least, the observation set Ω and the frequency support $W = \mathrm{supp}\ \hat{f}$ must overlap at one location; otherwise, all of the observations are zero, and nothing can be done. Choosing Ω

Authorized licensed use limited to: IEEE Xplore. Downloaded on December 30, 2008 at 06:05 from IEEE Xplore. Restrictions apply.

uniformly at random, the probability that it includes none of the members of W is

$$\boldsymbol{P}(\Omega \cap W = \emptyset) = \frac{\binom{N-\sqrt{N}}{|\Omega|}}{\binom{N}{|\Omega|}} \geq \left(1 - \frac{2|\Omega|}{N}\right)^{\sqrt{N}}$$

where we have used the assumption that $|\Omega| > |T| = \sqrt{N}$. Then for $\boldsymbol{P}(\Omega \cap W = \emptyset)$ to be smaller than N^{-M}, it must be true that

$$\sqrt{N} \cdot \log\left(1 - \frac{2|\Omega|}{N}\right) \leq -M \log N$$

and if we make the restriction that $|\Omega|$ cannot be as large as $N/2$, meaning that $\log\left(1 - \frac{2|\Omega|}{N}\right) \approx -\frac{2|\Omega|}{N}$, we have

$$|\Omega| \geq \text{Const} \cdot M \cdot \sqrt{N} \cdot \log N.$$

For the Dirac comb then, any algorithm must have $|\Omega| \sim |T| M \log N$ observations for the identified probability of success.

Examples for larger supports T exist as well. If N is an even power of two, we can superimpose 2^m Dirac combs at dyadic shifts to construct signals with time-domain support $|T| = 2^m\sqrt{N}$ and frequency-domain support $|W| = 2^{-m}\sqrt{N}$ for $m = 0, \ldots, \log_2 \sqrt{N}$. The same argument as above would then dictate that

$$|\Omega| \geq \text{Const} \cdot M \cdot \frac{N}{|W|} \cdot \log N = \text{Const} \cdot M \cdot |T| \cdot \log N.$$

In short, Theorem 1.3 identifies a fundamental limit. No recovery can be successful for all signals using significantly fewer observations.

E. Extensions

As mentioned earlier, results for our model problem extend easily to higher dimensions and alternate recovery scenarios. To be concrete, consider the problem of recovering a 1D piecewise-constant signal via

$$\min_{g} \sum_{t \in \mathbb{Z}_N} |g(t) - g(t-1)| \quad \text{subject to } \hat{g}|_\Omega = \hat{f}|_\Omega \qquad (1.7)$$

where we adopt the convention that $g(-1) = g(N-1)$. In a nutshell, model (1.5) is obtained from (1.7) after differentiation. Indeed, let δ be the vector of first difference $\delta(t) = g(t) - g(t-1)$, and note that $\sum \delta(t) = 0$. Obviously

$$\hat{\delta}(\omega) = (1 - e^{-2\pi i \omega/N})\hat{g}(\omega), \qquad \text{for all } \omega \neq 0$$

and, therefore, with $\upsilon(\omega) = (1 - e^{-2\pi i\omega/N})^{-1}$, the problem is identical to

$$\min_{\delta} ||\delta||_{\ell_1} \quad \text{s.t. } \hat{\delta}|_{\Omega\setminus\{0\}} = (\upsilon \hat{f})|_{\Omega\setminus\{0\}}, \quad \hat{\delta}(0) = 0$$

which is precisely what we have been studying.

Corollary 1.4: Put $T = \{t, f(t) \neq f(t-1)\}$. Under the assumptions of Theorem 1.3, the minimizer to the problem (1.7) is unique and is equal f with probability at least $1 - O(N^{-M})$—provided that f be adjusted so that $\sum f(t) = \hat{f}(0)$.

We now explore versions of Theorem 1.3 in higher dimensions. To be concrete, consider the 2D situation (statements in arbitrary dimensions are exactly of the same flavor).

Theorem 1.5: Put $N = n^2$. We let $f(t_1, t_2)$, $1 \leq t_1, t_2 \leq n$ be a discrete real-valued image and Ω of a certain size be chosen uniformly at random. Assume that for a given accuracy parameter M, f is supported on T obeying (1.6). Then with probability at least $1 - O(N^{-M})$, the minimizer to the problem (1.5) is unique and is equal to f.

We will not prove this result as the strategy is exactly parallel to that of Theorem 1.3. Letting $D_1 f$ be the horizontal finite differences $D_1 f(t_1, t_2) = f(t_1, t_2) - f(t_1 - 1, t_2)$ and $D_2 f$ be the vertical analog, we have just seen that we can think about the data as the properly renormalized Fourier coefficients of $D_1 f$ and $D_2 f$. Now put $d = D_1 f + i D_2 f$, where $i^2 = -1$. Then the minimum total-variation problem may be expressed as

$$\min ||\delta||_{\ell_1} \text{ subject to } F_\Omega \delta = F_\Omega d \qquad (1.8)$$

where F_Ω is a partial Fourier transform. One then obtains a statement for piecewise constant 2D functions, which is similar to that for sparse one–dimensional (1D) signals provided that the support of f be replaced by $\{(t_1, t_2) : |D_1 f(t_1, t_2)|^2 + |D_2 f(t_1, t_2)|^2 \neq 0\}$. We omit the details.

The main point here is that there actually are a variety of results similar to Theorem 1.3. Theorem 1.5 serves as another recovery example, and provides a precise quantitative understanding of the "surprising result" discussed at the beginning of this paper.

To be complete, we would like to mention that for complex valued signals, the minimum ℓ_1 problem (1.5) and, therefore, the minimum TV problem (1.1) can be recast as special convex programs known as second-order cone programs (SOCPs). For example, (1.8) is equivalent to

$$\begin{aligned} \min \quad & \sum_t u(t) \\ \text{subject to} \quad & \sqrt{|\delta_1(t)|^2 + |\delta_2(t)|^2} \leq u(t), \\ & F_\Omega(\delta_1 + i\delta_2) = F_\Omega d \end{aligned} \qquad (1.9)$$

with variables u, δ_1, and δ_2 in $\boldsymbol{R}^N$ (δ_1 and δ_2 are the real and imaginary parts of δ). If in addition, δ is real valued, then this is a linear program. Much progress has been made in the past decade on algorithms to solve both linear and second-order cone programs [6], and many off-the-shelf software packages exist for solving problems such as (P_1) and (1.9).

F. Relationship to Uncertainty Principles

From a certain point of view, our results are connected to the so-called *uncertainty principles* [4], [5] which say that it is difficult to localize a signal $f \in \boldsymbol{C}^N$ both in time and frequency

Authorized licensed use limited to: IEEE Xplore. Downloaded on December 30, 2008 at 06:05 from IEEE Xplore. Restrictions apply.

at the same time. Indeed, classical arguments show that f is the unique minimizer of (P_1) if and only if

$$\sum_{t\in\mathbb{Z}_N} |f(t)+h(t)| > \sum_{t\in\mathbb{Z}_N} |f(t)|, \quad \forall\, h \neq 0,\ \hat{h}|_\Omega = 0.$$

Put $T = \mathrm{supp}(f)$ and apply the triangle inequality

$$\begin{aligned}\sum_{\mathbb{Z}_N} |f(t)+h(t)| &= \sum_{T} |f(t)+h(t)| + \sum_{T^c} |h(t)| \\ &\geq \sum_{T} |f(t)| - |h(t)| + \sum_{T^c} |h(t)|.\end{aligned}$$

Hence, a sufficient condition to establish that f is our unique solution would be to show that

$$\sum_{T} |h(t)| < \sum_{T^c} |h(t)| \quad \forall\, h \neq 0,\ \hat{h}|_\Omega = 0$$

or, equivalently, $\sum_T |h(t)| < \frac{1}{2}||h||_{\ell_1}$. The connection with the uncertainty principle is now explicit; f is the unique minimizer if it is impossible to concentrate half of the ℓ_1 norm of a signal that is missing frequency components in Ω on a "small" set T. For example, [4] guarantees exact reconstruction if

$$2|T| \cdot (N - |\Omega|) < N.$$

Take $|\Omega| < N/2$, then that condition says that $|T|$ must be zero which is far from being the content of Theorem 1.3.

By refining these uncertainty principles, [7] shows that a much stronger recovery result is possible. The central results of [7] imply that a signal consisting of $|T|$ spikes which are spread out in a somewhat even manner in the time domain can be recovered from $C \cdot |T|$ lowpass observations. Theorem 1.3 is different in that it applies to *all* signals with a certain support size, and does not rely on a special choice of Ω (almost any Ω which is large enough will work). The price for this additional power is that we require a factor of $\log N$ more observations.

In truth, this paper does not follow this classical approach of deriving a recovery condition directly from an uncertainty principle. Instead, we will use duality theory to study the solution of (P_1). However, a byproduct of our analysis will be a novel uncertainty principle that holds for *generic* sets T, Ω.

G. Robust Uncertainty Principles

Underlying our results is a new notion of uncertainty principle which holds for almost any pair $(\mathrm{supp}(f), \mathrm{supp}(\hat{f}))$. With $T = \mathrm{supp}(f)$ and $\Omega = \mathrm{supp}(\hat{f})$, the classical discrete uncertainty principle [4] says that

$$|T| + |\Omega| \geq 2\sqrt{N} \tag{1.10}$$

with equality obtained for signals such as the Dirac comb. As we mentioned earlier, such extremal signals correspond to very special pairs (T, Ω). However, for most choices of T and Ω, the analysis presented in this paper shows that it is *impossible* to find f such that $T = \mathrm{supp}(f)$ and $\Omega = \mathrm{supp}(\hat{f})$ unless

$$|T| + |\Omega| \geq \gamma(M) \cdot (\log N)^{-1/2} \cdot N \tag{1.11}$$

which is considerably stronger than (1.10). Here, the statement "most pairs" says again that the probability of selecting a random pair (T, Ω) violating (1.11) is at most $O(N^{-M})$.

In some sense, (1.11) is the typical uncertainty relation one can generally expect (as opposed to (1.10)), hence, justifying the title of this paper. Because of space limitation, we are unable to elaborate on this fact and its implications further, but will do so in a companion paper.

H. Connections With Existing Work

The idea of relaxing a combinatorial problem into a convex problem is not new and goes back a long way. For example, [8], [9] used the idea of minimizing ℓ_1 norms to recover spike trains. The motivation is that this makes available a host of computationally feasible procedures. For example, a convex problem of the type (1.5) can be practically solved using techniques of linear programming such as interior point methods [10].

Using an ℓ_1 minimization program to recover sparse signals has been proposed in several different contexts. Early work in geophysics [9], [11], [12] centered on super-resolving spike trains from band-limited observations, i.e., the case where Ω consists of low-pass frequencies. Later works [4], [7] provided a unified framework in which to interpret these results by demonstrating that the effectiveness of recovery via minimizing ℓ_1 was linked to discrete uncertainty principles. As mentioned in Section I-F, these papers derived explicit bounds on the number of frequency samples needed to reconstruct a sparse signal. The earlier [4] also contains a conjecture that more powerful uncertainty principles may exist if one of T, Ω is chosen at random, which is essentially the content of Section I-G here.

More recently, there exists a series of beautiful papers [5], [13]–[16] concerned with problem of finding the sparsest decomposition of a signal f using waveforms from a highly overcomplete dictionary D. One seeks the sparsest α such that

$$f = D\alpha \tag{1.12}$$

where the number of columns M from D is greater than the sample size N. Consider the solution which minimizes the ℓ_0 norm of α subject to the constraint (1.12) and that which minimizes the ℓ_1 norm. A typical result of this body of work is as follows: suppose that s can be synthesized out of very few elements from D, then the solution to both problems are unique and are equal. We also refer to [17], [18] for very recent results along these lines.

This literature certainly influenced our thinking in the sense it made us suspect that results such as Theorem 1.3 were actually possible. However, we would like to emphasize that the claims presented in this paper are of a substantially different nature. We give essentially two reasons.

1) Our model problem is different since we need to "guess" a signal from incomplete data, as opposed to finding the sparsest expansion of a fully specified signal.
2) Our approach is decidedly probabilistic—as opposed to deterministic—and thus calls for very different techniques. For example, underlying our analysis are delicate estimates for the norms of certain types of random matrices, which may be of independent interest.

Authorized licensed use limited to: IEEE Xplore. Downloaded on December 30, 2008 at 06:05 from IEEE Xplore. Restrictions apply.

Apart from the wonderful properties of ℓ_1, several novel sampling theorems have been introduced in recent years. In [19], [20], the authors study universal sampling patters that allow the exact reconstruction of signals supported on a small set. In [21], ideas from spectral analysis are leveraged to show that a sequence of N_t spikes can be recovered exactly from $2N_t + 1$ consecutive Fourier samples (in [21], for example, the recovery requires solving a system of equations and factoring a polynomial). Our results, namely, Theorems 1.1 and 1.3 require slightly more samples to be taken ($C \cdot N_t \log N$ versus $C \cdot N_t$), but are again more general in that they address the radically different situation in which we do not have the freedom to choose the sample locations at our convenience.

Finally, it is interesting to note that our results and the references above are also related to recent work [22] in finding near-best B-term Fourier approximations (which is in some sense the dual to our recovery problem). The algorithm in [22], [23], which operates by estimating the frequencies present in the signal from a small number of randomly placed samples, produces with high probability an approximation in sublinear time with error within a constant of the best B-term approximation. First, in [23] the samples are again selected to be equispaced whereas we are not at liberty to choose the frequency samples at all since they are specified *a priori*. And second, we wish to produce as a result an entire signal or image of size N, so a sublinear algorithm is an impossibility.

I. Random Sensing

Against this background, the main contribution of this paper is the idea that one can use randomness as a sensing mechanism; that is, as a way of extracting information about an object of interest from a small number of randomly selected observations. For example, we have seen that if an object has a sparse gradient, then we can "image" this object by measuring a few Fourier samples at random locations, rather than by acquiring a large number of pixels.

This point of view is very broad. Suppose we wish to reconstruct a signal f assumed to be sparse in a fixed basis, e.g., a wavelet basis. Then by applying random sensing—taking a small number of random measurements—the number of measurement we need depends far more upon the *structural content* of the signal (the number of significant terms in the wavelet expansion) than the resolution N. From a quantitative viewpoint, our methodology should certainly be amenable to such general situations, as we will discuss further in Section VI-C.

II. Strategy

There exists at least one minimizer to (P_1) but it is not clear why this minimizer should be unique, and why it should equal f. In this section, we outline our strategy for answering these questions. In Section II-A, we use duality theory to show that f is the unique solution to (P_1) if and only if a trigonometric polynomial with certain properties exists (a similar duality approach was independently developed in [24] for finding sparse approximations from general dictionaries). We construct a special polynomial in Section II-B and the remainder of the paper is devoted to showing that if (1.6) holds, then our polynomial obeys the required properties.

A. Duality

Suppose that f is supported on T, and we observe $\hat{f}$ on a set Ω. The following lemma shows that a necessary and sufficient condition for the solution f to be the solution to (P_1) is the existence of a trigonometric polynomial P whose Fourier transform is supported on Ω, matches $\mathrm{sgn}(f)$ on T, and has magnitude strictly less than 1 elsewhere.

Lemma 2.1: Let $\Omega \subset \mathbb{Z}_N$. For a vector $f \in \boldsymbol{C}^N$ with $T := \mathrm{supp}(f)$, define the sign vector $\mathrm{sgn}(f)(t) := f(t)/|f(t)|$ when $t \in T$ and $\mathrm{sgn}(f) = 0$ otherwise. Suppose there exists a vector P whose Fourier transform $\hat{P}$ is supported in Ω such that

$$P(t) = \mathrm{sgn}(f)(t) \text{ for all } t \in T \tag{2.13}$$

and

$$|P(t)| < 1 \text{ for all } t \notin T. \tag{2.14}$$

Then if $\mathcal{F}_{T\to\Omega}$ is injective, the minimizer $f^\sharp$ to the problem (P_1) is unique and is equal to f. Conversely, if f is the unique minimizer of (P_1), then there exists a vector P with the above properties.

This is a result in convex optimization whose proof is given in the Appendix.

Since the space of functions with Fourier transform supported in Ω has $|\Omega|$ degrees of freedom, and the condition that P match $\mathrm{sgn}(f)$ on T requires $|T|$ degrees of freedom, one now expects heuristically (if one ignores the open conditions that P has magnitude strictly less than 1 outside of T) that $f^\sharp$ should be unique and be equal to f whenever $|T| \ll |\Omega|$; in particular, this gives an explicit procedure for recovering f from Ω and $\hat{f}|_\Omega$.

B. Architecture of the Argument

We will show that we can recover f supported on T from observations on almost all sets Ω obeying (1.6) by constructing a *particular* polynomial P (that depends on T and Ω) which automatically satisfies the equality constraints (2.13) on T, and then showing the inequality constraints (2.14) on T^c hold with high probability.

With $|\Omega| > |T|$, and if $\mathcal{F}_{T\to\Omega}$ is injective (has full column rank), there are many trigonometric polynomials supported on Ω in the Fourier domain which satisfy (2.13). We choose, with the hope that its magnitude on T^c is small, the one with minimum energy

$$P := \mathcal{F}_\Omega^* \mathcal{F}_{T\to\Omega} \left(\mathcal{F}_{T\to\Omega}^* \mathcal{F}_{T\to\Omega}\right)^{-1} \iota^* \mathrm{sgn}(f) \tag{2.15}$$

where $\mathcal{F}_\Omega = \mathcal{F}_{\boldsymbol{Z}_N\to\Omega}$ is the Fourier transform followed by a restriction to the set Ω; the embedding operator $\iota : \ell_2(T) \to \ell_2(\boldsymbol{Z}_N)$ extends a vector on T to a vector on $\boldsymbol{Z}_N$ by placing zeros outside of T; and ι^* is the dual restriction map $\iota^* f = f|_T$. It is easy to see that $\hat{P}$ is supported on Ω, and noting that $\iota^* \mathcal{F}_\Omega^* = \mathcal{F}_{T\to\Omega}^*$, P also satisfies (2.13)

$$\iota^* P = \iota^* \mathrm{sgn}(f).$$

Authorized licensed use limited to: IEEE Xplore. Downloaded on December 30, 2008 at 06:05 from IEEE Xplore. Restrictions apply.

Fixing f and its support T, we will prove Theorem 1.3 by establishing that if the set Ω is chosen uniformly at random from all sets of size $N_\omega \geq C_M^{-1} \cdot |T| \cdot \log N$, then

1) *Invertibility.* The operator $\mathcal{F}_{T\to\Omega}$ is injective, meaning that $\mathcal{F}^*_{T\to\Omega}\mathcal{F}_{T\to\Omega}$ in (2.15) is invertible, with probability $1 - O(N^{-M})$.
2) *Magnitude on T^c.* The function P in (2.15) obeys $|P(t)| < 1$ for all $t \in T^c$ again with probability $1 - O(N^{-M})$.

Making these arguments directly for the case where Ω of a certain size is chosen uniformly at random would be complicated, as the probability of a particular frequency being included in the set Ω would depend on whether or not each other frequency is included. To simplify the analysis, the next subsection introduces a Bernoulli probability model for selecting the set Ω, and shows how results using this model can be translated into results for the uniform probability model.

C. The Bernoulli Model

A set Ω' of Fourier coefficients is sampled using the Bernoulli model with parameter $0 < \tau < 1$ by first creating the sequence

$$I_\omega = \begin{cases} 0, & \text{with probability } 1-\tau \\ 1, & \text{with probability } \tau \end{cases} \tag{2.16}$$

and then setting

$$\Omega' := \{\omega : I_\omega = 1\}. \tag{2.17}$$

The size of the set $|\Omega'|$ is also random, following a binomial distribution, and $\boldsymbol{E}(|\Omega'|) = \tau N$. In fact, classical large deviations arguments tell us that as N gets large, $|\Omega'|/N \approx \tau$ with high probability.

With this pobability model, we establish two formal statements showing that P in (2.15) obeys the conditions of Lemma 2.1. Both are proven in Section III.

Theorem 2.2: Let T be a fixed subset, and choose Ω using the Bernoulli model with parameter τ. Suppose that

$$|T| \leq C_M \cdot (\log N)^{-1} \cdot \tau N \tag{2.18}$$

where C_M is the same as in Theorem 1.3. Then $\mathcal{F}^*_{T\to\Omega}\mathcal{F}_{T\to\Omega}$ is invertible with probability at least $1 - O(N^{-M})$.

Lemma 2.3: Under the assumptions of Theorem 2.2, P in (2.15) obeys $|P(t)| < 1$ for all $t \in T^c$ with probability at least $1 - O(N^{-M})$.

We now explain why these two claims give Theorem 1.3. Define $\mathrm{Failure}(\Omega_0)$ as the event where no dual polynomial P, supported on Ω_0 in the Fourier domain, exists that obeys the conditions (2.13) and (2.14) above. Let Ω of size N_ω be drawn using the uniform model, and let Ω' be drawn from the Bernoulli model with $\tau = N_\omega/N$. We have

$$\begin{aligned} \boldsymbol{P}(\mathrm{Failure}(\Omega')) &= \sum_{k=0}^{N} \boldsymbol{P}(\mathrm{Failure}(\Omega') \mid |\Omega'| = k)\, \boldsymbol{P}(|\Omega'| = k) \\ &= \sum_{k=0}^{N} \boldsymbol{P}(\mathrm{Failure}(\Omega_k))\, \boldsymbol{P}(|\Omega'| = k) \end{aligned}$$

where Ω_k is selected uniformly at random with $|\Omega_k| = k$. We make two observations.

- $\boldsymbol{P}(\mathrm{Failure}(\Omega_k))$ is a nonincreasing function of k. This follows directly from the fact that

$$\Omega_1 \subset \Omega_2 \Rightarrow \boldsymbol{P}(\mathrm{Failure}(\Omega_2)) \leq \boldsymbol{P}(\mathrm{Failure}(\Omega_1))$$

  (the larger Ω becomes, it only becomes easier to construct a valid P).
- Since τN is an integer, it is the median of $|\Omega'|$

$$\boldsymbol{P}(|\Omega'| \leq \tau N - 1) < 1/2 < \boldsymbol{P}(|\Omega'| \leq \tau N).$$

  (See [25] for a proof.)

With the above in mind, we continue

$$\begin{aligned} \boldsymbol{P}(\mathrm{Failure}(\Omega')) &\geq \sum_{k=1}^{N_\omega} \boldsymbol{P}(\mathrm{Failure}(\Omega_k)) \cdot \boldsymbol{P}(|\Omega'| = k) \\ &\geq \boldsymbol{P}(\mathrm{Failure}(\Omega)) \cdot \sum_{k=1}^{N_\omega} \boldsymbol{P}(|\,\Omega'| = k) \\ &\geq \frac{1}{2} \cdot \boldsymbol{P}(\mathrm{Failure}(\Omega)). \end{aligned}$$

Thus, if we can bound the probability of failure for the Bernoulli model, we know that the failure rate for the uniform model will be no more than twice as large.

III. Construction of the Dual Polynomial

The Bernoulli model holds throughout this section, and we carefully examine the minimum energy dual polynomial P defined in (2.15) and establish Theorem 2.2 and Lemma 2.3. The main arguments hinge on delicate moment bounds for random matrices, which are presented in Section IV. From here on forth, we will assume that $|\tau N| > M \log N$ since the claim is vacuous otherwise (as we will see, $C_M \leq 1/M$ and thus (1.6) will force $f \equiv 0$, at which point it is clear that the solution to (P_1) is equal to $f = 0$).

We will find it convenient to rewrite (2.15) in terms of the auxiliary matrix

$$Hf(t) := -\sum_{\omega\in\Omega} \sum_{t'\in T: t'\neq t} e^{2\pi i \frac{\omega(t-t')}{N}} f(t') \tag{3.19}$$

and define

$$H_0 = \iota^* H.$$

To see the relevance of the operators H and H_0, observe that

$$\begin{aligned} \iota - \frac{1}{|\Omega|} H &= \frac{1}{|\Omega|} \mathcal{F}^*_\Omega \mathcal{F}_{T\to\Omega} \\ I_T - \frac{1}{|\Omega|} H_0 &= \frac{1}{|\Omega|} \mathcal{F}^*_{T\to\Omega} \mathcal{F}_{T\to\Omega} \end{aligned}$$

where I_T is the identity for $\ell^2(T)$ (note that $\iota^*\iota = I_T$). Then

$$P = \left(\iota - \frac{1}{|\Omega|} H\right) \left(I_T - \frac{1}{|\Omega|} H_0\right)^{-1} \iota^* \mathrm{sgn} f.$$

Authorized licensed use limited to: IEEE Xplore. Downloaded on December 30, 2008 at 06:05 from IEEE Xplore. Restrictions apply.

The point here is to separate the constant diagonal of $\mathcal{F}^*_{T\to\Omega}\mathcal{F}_{T\to\Omega}$ (which is $|\Omega|$ everywhere) from the highly oscillatory off-diagonal. We will see that choosing Ω at random makes H_0 essentially a "noise" matrix, making $I_T - \frac{1}{|\Omega|}H_0$ well conditioned.

A. Invertibility

We would like to establish invertibility of the matrix $I_T - \frac{1}{|\Omega|}H_0$ with high probability. One way to proceed would be to show that the operator norm (i.e., the largest eigenvalue) of H_0 is less than $|\Omega|$. A straightforward way to do this is to bound the operator norm $\|H_0\|$ by the *Frobenius norm* $\|H_0\|_F$

$$\|H_0\|^2 \le \|H_0\|_F^2 := \mathrm{Tr}(H_0H_0^*) = \sum_{t_1,t_2} |(H_0)_{t_1,t_2}|^2 \quad (3.20)$$

where $(H_0)_{t_1,t_2}$ is the matrix element at row t_1 and column t_2.

Using relatively simple statistical arguments, we can show that with high probability $|(H_0)_{t_1,t_2}|^2 \sim |\Omega|$. Applying (3.20) would then yield invertibility when $|T| \sim \sqrt{|\Omega|}$. To show that H_0 is "small" for larger sets T (recall that $|T| \sim |\Omega|\cdot(\log N)^{-1}$ is the desired result), we use estimates of the Frobenius norm of a *large power* of H_0, taking advantage of cancellations arising from the randomness of the matrix coefficients of H_0.

Our argument relies on a key estimate which we introduce now and shall be discussed in greater detail in Section III-B. Assume that $\tau \le 1/(1+e)$ and $n \le \tau N/[4|T|(1-\tau)]$. Then the $2n$th moment of H_0 obeys

$$\boldsymbol{E}(\mathrm{Tr}(H_0^{2n})) \le 2\left(\frac{4}{e(1-\tau)}\right)^n n^{n+1}\cdot|\tau N|^n|T|^{n+1}. \quad (3.21)$$

Now this moment bound gives an estimate for the operator norm of H_0. To see this, note that since H_0 is self-adjoint

$$\|H_0\|^{2n} = \|H_0^n\|^2 \le \|H_0^n\|_F^2 = \mathrm{Tr}(H_0^{2n}).$$

Letting α be a positive number $0<\alpha<1$, it follows from the Markov inequality that

$$\boldsymbol{P}(\|H_0^n\|_F \ge \alpha^n\cdot|\tau N|^n) \le \frac{\boldsymbol{E}\,\|H_0^n\|_F^2}{\alpha^{2n}|\tau N|^{2n}}.$$

We then apply inequality (3.21) (recall $\|H_0^n\|_F^2 = \mathrm{Tr}(H_0^{2n})$) and obtain

$$\boldsymbol{P}(\|H_0^n\|_F \ge \alpha^n\cdot|\tau N|^n) \le 2ne^{-n}\left(\frac{4n}{\alpha^2(1-\tau)}\right)^n\left(\frac{|T|}{|\tau N|}\right)^n|T|. \quad (3.22)$$

We remark that the last inequality holds for any sample size $|T|$ (with the proviso that $n \le \tau N/[4|T|(1-\tau)]$) and we now specialize (3.22) to selected values of $|T|$.

Theorem 3.1: Assume that $\tau \le (1+e)^{-1}$ and suppose that T obeys

$$|T| \le \frac{\alpha_M^2(1-\tau)}{4}\frac{|\tau N|}{n}, \qquad \text{for some } \alpha_M \le \alpha \le 1. \quad (3.23)$$

Then

$$\boldsymbol{P}(\|H_0^n\|_F \ge \alpha^n\cdot|\tau N|^n) \le \frac{1}{2}\alpha^2e^{-n}|\tau N|. \quad (3.24)$$

Select $n = (M+1)\log N$ which corresponds to the assumptions of Theorem 2.2. Then the operator $I_T - \frac{1}{|\Omega|}H_0$ is invertible with probability at least $1 - 1.25N^{-M}$.

Proof: The first part of the theorem follows from (3.22). For the second part, we begin by observing that a typical application of the large deviation theorem gives

$$\boldsymbol{P}(|\Omega| < \boldsymbol{E}|\Omega| - t) \le \exp(-t^2/2\boldsymbol{E}|\Omega|). \quad (3.25)$$

Slightly more precise estimates are possible, see [26]. It then follows that

$$\boldsymbol{P}(|\Omega| < (1-\epsilon_M)|\tau N|) \le N^{-M} \quad (3.26)$$

where

$$\epsilon_M := \sqrt{\frac{2M\log N}{|\tau N|}}.$$

We will denote by B_M the event $\{|\Omega| < (1-\epsilon_M)|\tau N|\}$.

We now take $n = (M+1)\log N$ and $\alpha = 1/\sqrt{2}$ and assume that T obeys (3.23) (note that $|T|$ obeys the assumptions of Theorem 2.2). Put $A_M := \{\|H_0\| \ge |\tau N|/\sqrt{2}\}$. Then

$$\boldsymbol{P}(A_M) \le \frac{1}{4}\cdot|\tau N|\cdot N^{-(M+1)} \le \frac{1}{4}N^{-M}$$

and on the complement of $A_M \cup B_M$, we have

$$\|H_0\| \le \tau N/\sqrt{2} \le |\Omega|/[\sqrt{2}(1-\epsilon_M)].$$

Hence, $I_T - \frac{1}{|\Omega|}H_0$ is invertible with the desired probability. □

We have thus established Theorem 2.2, and thus P is well defined with high probability.

To conclude this section, we would like to emphasize that our analysis gives a rather precise estimate of the norm of H_0.

Corollary 3.2: Assume, for example, that $|T|\log|T| \le \tau N/(4(1-\tau))$ and set $\gamma = \sqrt{4/(1-\tau)}$. For any $\epsilon > 0$, we have

$$\boldsymbol{P}\left(\|H_0\| > (1+\epsilon)\gamma\sqrt{\log|T|}\sqrt{|T||\tau N|}\right) \to 0$$

as $|T|, |\tau N| \to \infty$.

Proof: Put $\lambda = \gamma\sqrt{\log|T|}\sqrt{|T||\tau N|}$. The Markov inequality gives

$$\boldsymbol{P}(\|H_0\| \ge (1+\epsilon)\lambda) \le \frac{\boldsymbol{E}\left[\mathrm{Tr}(H_0^{2n})\right]}{(1+\epsilon)^{2n}\lambda^{2n}}.$$

Select $n = \lceil\log|T|\rceil$ so that

$$e^{-n}n^n|T| \le \lceil\log|T|\rceil^n.$$

For this n, $\boldsymbol{E}[\mathrm{Tr}(H_0^{2n})] \le 2n\lambda^{2n}$ (3.21). Therefore, the probability is bounded by $2n(1+\epsilon)^{-2n}$ which goes to zero as $n = \lceil\log|T|\rceil$ goes to infinity. □

Authorized licensed use limited to: IEEE Xplore. Downloaded on December 30, 2008 at 06:05 from IEEE Xplore. Restrictions apply.

B. The Key Estimate

Our key estimate (3.21) is stated below. The proof is technical and deferred to Section IV.

Theorem 3.3: Let $\tau \leq 1/(1+e)$ and $n_0 = \frac{\tau N}{4(1-\tau)|T|}$. With the Bernoulli model, if $n \leq n_0$, then

$$\boldsymbol{E}(\mathrm{Tr}(H_0^{2n})) \leq 2\left(\frac{4}{e(1-\tau)}\right)^n n^{n+1}|\tau N|^n|T|^{n+1} \quad (3.27a)$$

and if $n > n_0$

$$\boldsymbol{E}(\mathrm{Tr}(H_0^{2n})) \leq \frac{n}{1-\tau}(4n)^{2n-1}|\tau N||T|^{2n}. \quad (3.27b)$$

In other words, when $n \leq \frac{\tau N}{4|T|(1-\tau)}$, the $2n$th moment obeys (3.21).

C. Magnitude of the Polynomial on the Complement of T

In the remainder of Section III, we argue that $\max_{t\notin T}|P(t)| < 1$ with high probability and prove Lemma 2.3. We first develop an expression for $P(t)$ by making use of the algebraic identity

$$(1-M)^{-1} = (1-M^n)^{-1}(1+M+\cdots+M^{n-1}).$$

Indeed, we can write

$$\left(I_T - \frac{1}{|\Omega|^n}H_0^n\right)^{-1} = I_T + R, \quad \text{where } R = \sum_{p=1}^{\infty}\frac{1}{|\Omega|^{pn}}H_0^{pn}$$

so that the inverse is given by the truncated Neumann series

$$\left(I_T - \frac{1}{|\Omega|}H_0\right)^{-1} = (I_T+R)\sum_{m=0}^{n-1}\frac{1}{|\Omega|^m}H_0^m. \quad (3.28)$$

The point is that the remainder term R is quite small in the Frobenius norm: suppose that $\|\iota^* H\|_F \leq \alpha\cdot|\Omega|$, then

$$\|R\|_F \leq \frac{\alpha^n}{1-\alpha^n}.$$

In particular, the matrix coefficients of R are all individually less than $\alpha^n/(1-\alpha^n)$. Introduce the ℓ_∞-norm of a matrix as $\|M\|_\infty = \sup_{\|x\|_\infty\leq 1}\|Mx\|_\infty$ which is also given by

$$\|M\|_\infty = \sup_i \sum_j |M(i,j)|.$$

It follows from the Cauchy–Schwarz inequality that

$$\|M\|_\infty^2 \leq \sup_i \#\mathrm{col}(M)\sum_j |M(i,j)|^2 \leq \#\mathrm{col}(M)\cdot\|M\|_F^2$$

where by $\#\mathrm{col}(M)$ we mean the number of columns of M. This observation gives the crude estimate

$$\|R\|_\infty \leq |T|^{1/2}\cdot\frac{\alpha^n}{1-\alpha^n}. \quad (3.29)$$

As we shall soon see, the bound (3.29) allows us to effectively neglect the R term in this formula; the only remaining difficulty will be to establish good bounds on the truncated Neumann series $\frac{1}{|\Omega|}H\sum_{m=0}^{n-1}\frac{1}{|\Omega|^m}H_0^m$.

D. Estimating the Truncated Neumann Series

From (2.15) we observe that on the complement of T

$$P = \frac{1}{|\Omega|}H\left(I_T - \frac{1}{|\Omega|}H_0\right)^{-1}\iota^*\mathrm{sgn}(f)$$

since the ι component in (2.15) vanishes outside of T. Applying (3.28), we may rewrite P as

$$P(t) = P_0(t) + P_1(t), \quad \forall\, t\in T^c,$$

where

$$P_0 = S_n\mathrm{sgn}(f)$$
$$P_1 = \frac{1}{|\Omega|}HR\iota^*(I+S_{n-1})\mathrm{sgn}(f)$$

and

$$S_n = \sum_{m=1}^{n}|\Omega|^{-m}(H\iota^*)^m.$$

Let $a_0, a_1 > 0$ be two numbers with $a_0 + a_1 = 1$. Then

$$\boldsymbol{P}\left(\sup_{t\in T^c}|P(t)|>1\right) \leq \boldsymbol{P}(\|P_0\|_\infty > a_0) + \boldsymbol{P}(\|P_1\|_\infty > a_1)$$

and the idea is to bound each term individually. Put $Q_0 = S_{n-1}\mathrm{sgn}(f)$ so that $P_1 = \frac{1}{|\Omega|}HR\iota^*(\mathrm{sgn}(f)+Q_0)$. With these notations, observe that

$$\|P_1\|_\infty \leq \frac{1}{|\Omega|}\|HR\|_\infty\left(1+\|\iota^*Q_0\|_\infty\right).$$

Hence, bounds on the magnitude of P_1 will follow from bounds on $\|HR\|_\infty$ together with bounds on the magnitude of ι^*Q_0. It will be sufficient to derive bounds on $\|Q_0\|_\infty$ (since $\|\iota^*Q_0\|_\infty \leq \|Q_0\|_\infty$) which will follow from those on P_0 since Q_0 is nearly equal to P_0 (they differ by only one very small term).

Fix $t\in T^c$ and write $P_0(t)$ as

$$P_0(t) = \sum_{m=1}^{n}|\Omega|^{-m}X_m(t), \quad X_m = (H\iota^*)^m\mathrm{sgn}(f).$$

The idea is to use moment estimates to control the size of each term $X_m(t)$.

Lemma 3.4: Set $n = km$. Then $\boldsymbol{E}|X_m(t_0)|^{2k}$ obeys the same estimate as that in Theorem 3.3 (up to a multiplicative factor $|T|^{-1}$), namely

$$\boldsymbol{E}|X_m(t_0)|^{2k} \leq \frac{1}{|T|}B_n \quad (3.30)$$

Authorized licensed use limited to: IEEE Xplore. Downloaded on December 30, 2008 at 06:05 from IEEE Xplore. Restrictions apply.

where B_n is the right-hand side of (3.27). In particular, following (3.21)

$$\boldsymbol{E}|X_m(t_0)|^{2k} \le 2e^{-n}(4/(1-\tau))^n n^{n+1} \cdot |T|^n |\tau N|^n \quad (3.31)$$

provided that $n \le \frac{\tau N}{4|T|(1-\tau)}$.

The proof of these moment estimates mimics that of Theorem 3.3 and may be found in the Appendix.

Lemma 3.5: Fix $a_0 = 0.91$. Suppose that $|T|$ obeys (3.23) and let B_M be the set where $|\Omega| < (1-\epsilon_M)\cdot|\tau N|$ with ϵ_M as in (3.26). For each $t \in \mathbb{Z}_N$, there is a set A_t with the property

$$\boldsymbol{P}(A_t) > 1-\epsilon_n, \qquad \epsilon_n = 2(1-\epsilon_M)^{-2n} n^2 e^{-n} \alpha^{2n} (0.42)^{-2n}$$

and

$$|P_0(t)| < 0.91, \ \ |Q_0(t)| < 0.91 \text{ on } A_t \cap B_M^c.$$

As a consequence

$$\boldsymbol{P}\left(\sup_t |P_0(t)| > a_0\right) \le N^{-M} + N\epsilon_n$$

and similarly for Q_0.

Proof: We suppose that n is of the form $n = 2^J - 1$ (this property is not crucial and only simplifies our exposition). For each m and k such that $km \ge n$, it follows from (3.23) and (3.31) together with some simple calculations that

$$\boldsymbol{E}|X_m(t)|^{2k} \le 2ne^{-n}\alpha^{2n} \cdot |\tau N|^{2n}. \quad (3.32)$$

Again, $|\Omega| \approx |\tau N|$ and we will develop a bound on the set B_M^c where $|\Omega| \ge (1-\epsilon_M)|\tau N|$. On this set

$$|P_0(t)| \le \sum_{m=1}^n Y_m, \qquad Y_m = \frac{1}{(1-\epsilon_M)^m |\tau N|^m} |X_m(t)|.$$

Fix $\beta_j > 0$, $0 \le j < J$, such that $\sum_{j=0}^{J-1} 2^j \beta_j \le a_0$. Obviously

$$\boldsymbol{P}\left(\sum_{m=1}^n Y_m > a_0\right) \le \sum_{j=0}^{J-1} \sum_{m=2^j}^{2^{j+1}-1} \boldsymbol{P}(Y_m > \beta_j) \le \sum_{j=0}^{J-1} \sum_{m=2^j}^{2^{j+1}-1} \beta_j^{-2K_j} \boldsymbol{E}|Y_m|^{2K_j}$$

where $K_j = 2^{J-j}$. Observe that for each m with $2^j \le m < 2^{j+1}$, $K_j m$ obeys $n \le K_j m < 2n$ and, therefore, (3.32) gives

$$\boldsymbol{E}|Y_m|^{2K_j} \le (1-\epsilon_M)^{-2n} \cdot (2ne^{-n}\alpha^{2n}).$$

For example, taking $\beta_j^{-K_j}$ to be constant for all j, i.e., equal to β_0^{-n}, gives

$$\boldsymbol{P}\left(\sum_{m=1}^n Y_m > a_0\right) \le 2(1-\epsilon_M)^{-2n} \cdot n^2 e^{-n} \alpha^{2n} \cdot \beta_0^{-2n}$$

with $\sum_{j=0}^{J-1} 2^j \beta_j \le a_0$. Numerical calculations show that for $\beta_0 = 0.42$, $\sum_j 2^j \beta_j \le 0.91$ which gives

$$\boldsymbol{P}\left(\sum_{m=1}^n Y_m > 0.91\right) \le 2(1-\epsilon_M)^{-2n} \cdot n^2 e^{-n} \alpha^{2n} \cdot (0.42)^{-2n}. \quad (3.33)$$

The claim for Q_0 is identical and the lemma follows. □

Lemma 3.6: Fix $a_1 = 0.09$. Suppose that the pair (α, n) obeys $|T|^{3/2} \frac{\alpha^n}{1-\alpha^n} \le a_1/2$. Then

$$\|P_1\|_\infty \le a_1$$

on the event $A \cap \{\|\iota^* H\|_F \le \alpha|\Omega|\}$, for some A obeying $\boldsymbol{P}(A) \ge 1 - O(N^{-M})$.

Proof: As we observed before, 1) $\|P_1\|_\infty \le \|H\|_\infty \|R\|_\infty (1 + \|Q_0\|_\infty)$, and 2) Q_0 obeys the bound stated in Lemma 3.5. Consider then the event $\{\|Q_0\|_\infty \le 1\}$. On this event, $\|P_1\| \le a_1$ if $\frac{1}{|\Omega|}\|H\|_\infty \|R\|_\infty \le a_1/2$. The matrix H obeys $\frac{1}{|\Omega|}\|H\|_\infty \le |T|$ since H has $|T|$ columns and each matrix element is bounded by $|\Omega|$ (note that far better bounds are possible). It then follows from (3.29) that

$$\|H\|_\infty \cdot \|R\|_\infty \le |T|^{3/2} \cdot \frac{\alpha^n}{1-\alpha^n}$$

with probability at least $1 - O(N^{-M})$. We then simply need to choose α and n such that the right-hand side is less than $a_1/2$. □

E. Proof of Lemma 2.3

We have now assembled all the intermediate results to prove Lemma 2.3 (and hence our main theorem). Indeed, we proved that $|P(t)| < 1$ for all $t \in T^c$ (again with high probability), provided that α and n be selected appropriately as we now explain.

Fix $M > 0$. We choose $\alpha = .42(1-\epsilon_M)$, where ϵ_M is taken as in (3.26), and n to be the nearest integer to $(M+1)\log N$.

1) With this special choice, $\epsilon_n = 2[(M+1)\log N]^2 \cdot N^{-(M+1)}$ and, therefore, Lemma 3.5 implies that both P_0 and Q_0 are bounded by 0.91 outside of T^c with probability at least $1 - [1 + 2((M+1)\log N)^2] \cdot N^{-M}$.
2) Lemma 3.6 assures that it is sufficient to have $N^{3/2}\alpha^n/(1-\alpha^n) \le 0.045$ to have $|P_1(t)| < 0.09$ on T^c. Because $\log(0.42) \approx -0.87$ and $\log(0.045) \approx -3.10$, this condition is approximately equivalent to

$$(1.5 - 0.87(M+1))\log N \le -3.10.$$

Take $M \ge 2$, for example; then the above inequality is satisfied as soon as $N \ge 17$.

To conclude, Lemma 2.3 holds with probability exceeding $1 - O([(M+1)\log N)^2] \cdot N^{-M})$ if T obeys

$$|T| \le C_M \cdot \frac{|\tau N|}{\log N}, \quad C_M = \frac{.42^2(1-\tau)}{4(M+1)}(1+o(1)).$$

Authorized licensed use limited to: IEEE Xplore. Downloaded on December 30, 2008 at 06:05 from IEEE Xplore. Restrictions apply.

In other words, we may take C_M in Theorem 1.3 to be of the form

$$C_M = \frac{1-\tau}{22.6(M+1)}(1+o(1)). \tag{3.34}$$

IV. Moments of Random Matrices

This section is devoted entirely to proving Theorem 3.3 and it may be best first to sketch how this is done. We begin in Section IV-A by giving a preliminary expansion of the quantity $\boldsymbol{E}(\mathrm{Tr}(H_0^{2n}))$. However, this expansion is not easily manipulated, and needs to be rearranged using the inclusion–exclusion formula, which we do in Section IV-B, and some elements of combinatorics (the Stirling number identities) which we give in Section IV-C. This allows us to establish a second, more usable, expansion for $\boldsymbol{E}(\mathrm{Tr}(H_0^{2n}))$ in Section IV-D. The proof of the theorem then proceeds by developing a recursive inequality on the central term in this second expansion, which is done in Section IV-E.

Before we begin, we wish to note that the study of the eigenvalues of operators like H_0 has a bit of historical precedence in the information theory community. Note that $I_T - H_0$ is essentially the composition of three projection operators; one that "time limits" a function to T, followed by a "bandlimiting" to Ω, followed by a final restriction to T. The distribution of the eigenvalues of such operators was studied by Landau and others [27]–[29] while developing the prolate spheroidal wave functions that are now commonly used in signal processing and communications. This distribution was inferred by examining the trace of large powers of this operator (see [29] in particular), much as we will do here.

A. First Formula for the Expected Value of the Trace of $(H_0)^{2n}$

Recall that $H_0(t,t'), t,t' \in T$, is the $|T| \times |T|$ matrix whose entries are defined by

$$H_0(t,t') = \begin{cases} 0, & t = t' \\ c(t-t'), & t \neq t' \end{cases} \quad c(u) = \sum_{\omega \in \Omega} e^{\frac{2\pi i}{N}\omega u}. \tag{4.35}$$

A diagonal element of the $2n$th power of H_0 may be expressed as

$$H_0^{2n}(t_1,t_1) = \sum_{t_2,\ldots,t_{2n}:t_j \neq t_{j+1}} c(t_1-t_2)\ldots c(t_{2n}-t_1)$$

where we adopt the convention that $t_{2n+1} = t_1$ whenever convenient and, therefore,

$$\boldsymbol{E}\left(\mathrm{Tr}\left(H_0^{2n}\right)\right) = \sum_{t_1,\ldots,t_{2n}:t_j \neq t_{j+1}} \boldsymbol{E}\left[\sum_{\omega_1,\ldots,\omega_{2n} \in \Omega} e^{\frac{2\pi i}{N}\sum_{j=1}^{2n}\omega_j(t_j - t_{j+1})}\right].$$

Using (2.17) and linearity of expectation, we can write this as

$$\sum_{t_1,\ldots,t_{2n}:t_j \neq t_{j+1}} \sum_{0 \leq \omega_1,\ldots,\omega_{2n} \leq N-1} e^{\frac{2\pi i}{N}\sum_{j=1}^{2n}\omega_j(t_j - t_{j+1})} \times \boldsymbol{E}\left[\prod_{j=1}^{2n} I_{\{\omega_j \in \Omega\}}\right].$$

The idea is to use the independence of the $I_{\{\omega_j \in \Omega\}}$'s to simplify this expression substantially; however, one has to be careful with the fact that some of the ω_j's may be the same, at which point one loses independence of those indicator variables. These difficulties require a certain amount of notation. We let $\mathbb{Z}_N = \{0,1,\ldots,N-1\}$ be the set of all frequencies as before, and let A be the finite set $A := \{1,\ldots,2n\}$. For all $\boldsymbol{\omega} := (\omega_1,\ldots,\omega_{2n})$, we define the equivalence relation $\sim_{\boldsymbol{\omega}}$ on A by saying that $j \sim_{\boldsymbol{\omega}} j'$ if and only if $\omega_j = \omega_{j'}$. We let $\mathcal{P}(A)$ be the set of all equivalence relations on A. Note that there is a partial ordering on the equivalence relations as one can say that $\sim_1 \leq \sim_2$ if $\sim_1$ is coarser than $\sim_2$, i.e., $a \sim_2 b$ implies $a \sim_1 b$ for all $a,b \in A$. Thus, the coarsest element in $\mathcal{P}(A)$ is the trivial equivalence relation in which all elements of A are equivalent (just one equivalence class), while the finest element is the equality relation $=$, i.e., each element of A belongs to a distinct class ($|A|$ equivalence classes).

For each equivalence relation $\sim$ in $\mathcal{P}$, we can then define the sets $\Omega(\sim) \subset \mathbb{Z}_N^{2n}$ by

$$\Omega(\sim) := \{\boldsymbol{\omega} \in \mathbb{Z}_N^{2n} : \sim_{\boldsymbol{\omega}} = \sim\}$$

and the sets $\Omega_{\leq}(\sim) \subset \mathbb{Z}_N^{2n}$ by

$$\Omega_{\leq}(\sim) := \bigcup_{\sim' \in \mathcal{P}:\sim' \leq \sim} \Omega(\sim') = \left\{\boldsymbol{\omega} \in \mathbb{Z}_N^{2n} : \sim_{\boldsymbol{\omega}} \leq \sim\right\}.$$

Thus, the sets $\{\Omega(\sim) : \sim \in \mathcal{P}\}$ form a partition of $\mathbb{Z}_N^{2n}$. The sets $\Omega_{\leq}(\sim)$ can also be defined as

$$\Omega_{\leq}(\sim) := \left\{\boldsymbol{\omega} \in \mathbb{Z}_N^{2n} : \omega_a = \omega_b \text{ whenever } a \sim b\right\}.$$

For comparison, the sets $\Omega(\sim)$ can be defined as

$$\Omega(\sim) := \left\{\boldsymbol{\omega} \in \mathbb{Z}_N^{2n} : \omega_a = \omega_b \text{ whenever } a \sim b, \text{ and } \omega_a \neq \omega_b \text{ whenever } a \not\sim b\right\}.$$

We give an example: suppose $n = 2$ and fix $\sim$ such that $1 \sim 4$ and $2 \sim 3$ (exactly two equivalence classes); then

$$\Omega(\sim) := \{\boldsymbol{\omega} \in \mathbb{Z}_N^4 : \omega_1 = \omega_4, \omega_2 = \omega_3, \text{ and } \omega_1 \neq \omega_2\}$$

while

$$\Omega_{\leq}(\sim) := \{\boldsymbol{\omega} \in \mathbb{Z}_N^4 : \omega_1 = \omega_4, \omega_2 = \omega_3\}.$$

Now, let us return to the computation of the expected value. Because the random variables I_k in (2.16) are independent and

Authorized licensed use limited to: IEEE Xplore. Downloaded on December 30, 2008 at 06:05 from IEEE Xplore. Restrictions apply.

have all the same distribution, the quantity $\boldsymbol{E}\left[\prod_{j=1}^{2n} I_{\omega_j}\right]$ depends only on the equivalence relation $\sim_{\boldsymbol{\omega}}$ and not on the value of $\boldsymbol{\omega}$ itself. Indeed, we have

$$\boldsymbol{E}\left(\prod_{j=1}^{2n} I_{\omega_j}\right) = \tau^{|A/\sim|}$$

where $A/\sim$ denotes the equivalence classes of $\sim$. Thus, we can rewrite the preceding expression as (4.36) at the bottom of the page, where $\sim$ ranges over all equivalence relations.

We would like to pause here and consider (4.36). Take $n = 1$, for example. There are only two equivalent classes on $\{1,2\}$ and, therefore, the right-hand side is equal to

$$\sum_{t_1,t_2:t_1\neq t_2}\left[\tau\sum_{(\omega_1,\omega_2)\in\mathbb{Z}_N^2:\omega_1=\omega_2} e^{\frac{2\pi i}{N}\omega_1(t_1-t_1)} + \tau^2\sum_{(\omega_1,\omega_2)\in\mathbb{Z}_N^2:\omega_1\neq\omega_2} e^{\frac{2\pi i}{N}\omega_1(t_1-t_2)+i\omega_2(t_2-t_1)}\right].$$

Our goal is to rewrite the expression inside the brackets so that the exclusion $\omega_1 \neq \omega_2$ does not appear any longer, i.e., we would like to rewrite the sum over $\boldsymbol{\omega}\in\mathbb{Z}_N^2 : \omega_1\neq\omega_2$ in terms of sums over $\boldsymbol{\omega}\in\mathbb{Z}_N^2 : \omega_1 = \omega_2$, and over $\boldsymbol{\omega}\in\mathbb{Z}_N^2$. In this special case, this is quite easy as

$$\sum_{\boldsymbol{\omega}\in\mathbb{Z}_N^2:\omega_1\neq\omega_2} = \sum_{\boldsymbol{\omega}\in\mathbb{Z}_N^2} - \sum_{\boldsymbol{\omega}\in\mathbb{Z}_N^2:\omega_1=\omega_2}.$$

The motivation is as follows: removing the exclusion allows to rewrite sums as product, e.g.,

$$\sum_{\boldsymbol{\omega}\in\mathbb{Z}_N^2} = \sum_{\omega_1} e^{\frac{2\pi i}{N}\omega_1(t_1-t_2)}\sum_{\omega_2} e^{\frac{2\pi i}{N}\omega_2(t_2-t_1)};$$

and each factor is equal to either N or 0 depending on whether $t_1 = t_2$ or not.

Section IV-B generalizes these ideas and develops an identity, which allows us to rewrite sums over $\Omega(\sim)$ in terms of sums over $\Omega_{\leq}(\sim)$.

B. Inclusion–Exclusion Formulae

Lemma 4.1: (*Inclusion–exclusion principle for equivalence classes*) Let A and G be nonempty finite sets. For any equivalence class $\sim\in\mathcal{P}(A)$ on $\boldsymbol{\omega}\in G^{|A|}$, we have

$$\sum_{\boldsymbol{\omega}\in\Omega(\sim)} f(\boldsymbol{\omega}) = \sum_{\sim_1\in\mathcal{P}:\sim_1\leq\sim} (-1)^{|A/\sim|-|A/\sim_1|} \times\left(\prod_{A'\in A/\sim_1}(|A'/\sim|-1)!\right)\sum_{\boldsymbol{\omega}\in\Omega_{\leq}(\sim_1)} f(\boldsymbol{\omega}). \quad (4.37)$$

Thus, for instance, if $A = \{1,2,3\}$ and $\sim$ is the equality relation, i.e., $j\sim k$ if and only if $j = k$, this identity is saying that

$$\sum_{\omega_1,\omega_2,\omega_3\in G:\omega_1,\omega_2,\omega_3\,\text{distinct}} = \sum_{\omega_1,\omega_2,\omega_3\in G} - \sum_{\omega_1,\omega_2,\omega_3:\omega_1=\omega_2} - \sum_{\omega_1,\omega_2,\omega_3\in G:\omega_2=\omega_3} - \sum_{\omega_1,\omega_2,\omega_3\in G:\omega_3=\omega_1} + 2\sum_{\omega_1,\omega_2,\omega_3\in G:\omega_1=\omega_2=\omega_3}$$

where we have omitted the summands $f(\omega_1,\omega_2,\omega_3)$ for brevity.

Proof: By passing from A to the quotient space $A/\sim$ if necessary we may assume that $\sim$ is the equality relation $=$. Now relabeling A as $\{1,\ldots,n\}$, $\sim_1$ as $\sim$, and A' as A, it suffices to show that

$$\sum_{\boldsymbol{\omega}\in G^n:\omega_1,\ldots,\omega_n\,\text{distinct}} f(\boldsymbol{\omega}) = \sum_{\sim\in\mathcal{P}(\{1,\ldots,n\})} (-1)^{n-|\{1,\ldots,n\}/\sim|} \times\left[\prod_{A\in\{1,\ldots,n\}/\sim}(|A|-1)!\right]\sum_{\boldsymbol{\omega}\in\Omega_{\leq}(\sim)} f(\boldsymbol{\omega}). \quad (4.38)$$

We prove this by induction on n. When $n = 1$ both sides are equal to $\sum_{\boldsymbol{\omega}\in G} f(\boldsymbol{\omega})$. Now suppose inductively that $n > 1$ and the claim has already been proven for $n-1$. We observe that the left-hand side of (4.38) can be rewritten as

$$\sum_{\boldsymbol{\omega}'\in G^{n-1}:\omega_1,\ldots,\omega_{n-1}\,\text{distinct}}\left[\sum_{\omega_n\in G} f(\boldsymbol{\omega}',\omega_n) - \sum_{j=1}^{n-1} f(\boldsymbol{\omega}',\omega_j)\right]$$

where $\boldsymbol{\omega}' := (\omega_1,\ldots,\omega_{n-1})$. Applying the inductive hypothesis, this can be written as

$$\sum_{\sim'\in\mathcal{P}(\{1,\ldots,n-1\})} (-1)^{n-1-|\{1,\ldots,n-1\}/\sim'|} \times\prod_{A'\in\{1,\ldots,n-1\}/\sim}(|A'|-1)! \times\sum_{\boldsymbol{\omega}'\in\Omega_{\leq}(\sim')}\left[\sum_{\omega_n\in G} f(\boldsymbol{\omega}',\omega_n) - \sum_{1\leq j\leq n} f(\boldsymbol{\omega}',\omega_j)\right]. \quad (4.39)$$

Now we work on the right-hand side of (4.38). If $\sim$ is an equivalence class on $\{1,\ldots,n\}$, let $\sim'$ be the restriction of $\sim$ to $\{1,\ldots,n-1\}$. Observe that $\sim$ can be formed from $\sim'$ either by adjoining the singleton set $\{n\}$ as a new equivalence class (in which case we write $\sim = \{\sim',\{n\}\}$, or by choosing a $j\in\{1,\ldots,n-1\}$ and declaring n to be equivalent to j (in which case we write $\sim = \{\sim',\{n\}\}/(j=n)$). Note that the

$$\boldsymbol{E}\left(\mathrm{Tr}\left(H_0^{2n}\right)\right) = \sum_{t_1,\ldots,t_{2n}:t_j\neq t_{j+1}}\sum_{\sim\in\mathcal{P}(A)}\left[\tau^{|A/\sim|}\sum_{\boldsymbol{\omega}\in\Omega(\sim)} e^{\frac{2\pi i}{N}\sum_{j=1}^{2n}\omega_j(t_j-t_{j+1})}\right] \quad (4.36)$$

Authorized licensed use limited to: IEEE Xplore. Downloaded on December 30, 2008 at 06:05 from IEEE Xplore. Restrictions apply.

latter construction can recover the same equivalence class $\sim$ in multiple ways if the equivalence class $[j]_{\sim'}$ of j in $\sim'$ has size larger than 1, however, we can resolve this by weighting each j by $\frac{1}{|[j]_{\sim'}|}$. Thus, we have the identity

$$\sum_{\sim\in\mathcal{P}(\{1,\ldots,n\})} F(\sim) = \sum_{\sim'\in\mathcal{P}(\{1,\ldots,n-1\})} F(\{\sim',\{n\}\}) + \sum_{\sim'\in\mathcal{P}(\{1,\ldots,n-1\})}\sum_{j=1}^{n-1}\frac{1}{|[j]_{\sim'}|}F(\{\sim',\{n\}\}/(j=n))$$

for any complex-valued function F on $\mathcal{P}(\{1,\ldots,n\})$. Applying this to the right-hand side of (4.38), we see that we may rewrite this expression as the sum of

$$\sum_{\sim'\in\mathcal{P}(\{1,\ldots,n-1\})} (-1)^{n-(|\{1,\ldots,n-1\}/\sim'|+1)} \times \left[\prod_{A\in\{1,\ldots,n-1\}/\sim'}(|A|-1)!\right]\sum_{\boldsymbol{\omega}'\in\Omega_{\leq}(\sim')} f(\boldsymbol{\omega}',\omega_n)$$

and

$$\sum_{\sim'\in\mathcal{P}(\{1,\ldots,n-1\})} (-1)^{n-|\{1,\ldots,n-1\}/\sim'|}\sum_{j=1}^{n-1}T(j) \times \sum_{\boldsymbol{\omega}'\in\Omega_{\leq}(\sim')} f(\boldsymbol{\omega}',\omega_j)$$

where we adopt the convention $\boldsymbol{\omega}' = (\omega_1,\ldots,\omega_{n-1})$. But observe that

$$T(j) := \frac{1}{|[j]_{\sim'}|}\prod_{A\in\{1,\ldots,n\}/(\{\sim',\{n\}\}/(j=n))}(|A|-1)! = \prod_{A'\in\{1,\ldots,n-1\}/\sim'}(|A'|-1)!$$

and thus the right-hand side of (4.38) matches (4.39) as desired. □

C. Stirling Numbers

As emphasized earlier, our goal is to use our inclusion–exclusion formula to rewrite the sum (4.36) as a sum over $\Omega_{\leq}(\sim)$. In order to do this, it is best to introduce another element of combinatorics, which will prove to be very useful.

For any $n,k\geq 0$, we define the Stirling number of the second kind $S(n,k)$ to be the number of equivalence relations on a set of n elements which have exactly k equivalence classes, thus,

$$S(n,k) := \#\{\sim\in\mathcal{P}(A) : |A/\sim| = k\}.$$

Thus, for instance, $S(0,0)=S(1,1)=S(2,1)=S(2,2)=1$, $S(3,2)=3$, and so forth. We observe the basic recurrence

$$S(n+1,k) = S(n,k-1)+kS(n,k) \text{ for all } k,n\geq 0. \quad (4.40)$$

This simply reflects the fact that if a is an element of A and $\sim$ is an equivalence relation on A with k equivalence classes, then either a is not equivalent to any other element of A (in which case $\sim$ has $k-1$ equivalence classes on $A\backslash\{a\}$), or a is equivalent to one of the k equivalence classes of $A\backslash\{a\}$.

We now need an identity for the Stirling numbers.[1]

Lemma 4.2: For any $n\geq 1$ and $0\leq\tau<1/2$, we have the identity

$$\sum_{k=1}^{n}(k-1)!S(n,k)(-1)^{n-k}\tau^k = \sum_{k=1}^{\infty}(-1)^{n-k}\frac{\tau^k k^{n-1}}{(1-\tau)^k}. \quad (4.41)$$

Note that the condition $0\leq\tau<1/2$ ensures that the right-hand side is convergent.

Proof: We prove this by induction on n. When $n=1$ the left-hand side is equal to τ, and the right-hand side is equal to

$$\sum_{k=1}^{\infty}(-1)^{k+1}\frac{\tau^k}{(1-\tau)^k} = -\sum_{k=0}^{\infty}\left(\frac{\tau}{\tau-1}\right)^k+1 = \frac{-1}{1-\frac{\tau}{\tau-1}}+1=\tau$$

as desired. Now suppose inductively that $n\geq 1$ and the claim has already been proven for n. Applying the operator $(\tau^2-\tau)\frac{d}{d\tau}$ to both sides (which can be justified by the hypothesis $0\leq\tau<1/2$) we obtain (after some computation)

$$\sum_{k=1}^{n+1}(k-1)!(S(n,k-1)+kS(n,k))(-1)^{n+1-k}\tau^k = \sum_{k=0}^{\infty}(-1)^{n+1-k}\frac{\tau^k k^n}{(1-\tau)^k}$$

and the claim follows from (4.40). □

We shall refer to the quantity in (4.41) as $F_n(\tau)$, thus,

$$F_n(\tau) = \sum_{k=1}^{n}(k-1)!S(n,k)(-1)^{n-k}\tau^k = \sum_{k=1}^{\infty}(-1)^{n+k}\frac{\tau^k k^{n-1}}{(1-\tau)^k}. \quad (4.42)$$

Thus, we have

$$F_1(\tau)=\tau,\quad F_2(\tau)=-\tau+\tau^2,\quad F_3(\tau)=\tau-3\tau^2+2\tau^3$$

and so forth. When τ is small, we have the approximation $F_n(\tau)\approx(-1)^{n+1}\tau$, which is worth keeping in mind. Some more rigorous bounds in this spirit are as follows.

Lemma 4.3: Let $n\geq 1$ and $0\leq\tau<1/2$. If $\frac{\tau}{1-\tau}\leq e^{1-n}$, then we have $|F_n(\tau)|\leq\frac{\tau}{1-\tau}$. If instead $\frac{\tau}{1-\tau}>e^{1-n}$, then

$$|F_n(\tau)|\leq e^{(n-1)\left(\log(n-1)-\log\log\frac{1-\tau}{\tau}-1\right)}.$$

Proof: Elementary calculus shows that for $x>0$, the function $g(x)=\frac{\tau^x x^{n-1}}{(1-\tau)^x}$ is increasing for $x<x_*$ and decreasing for $x>x^*$, where

$$x_* := (n-1)/\log\frac{1-\tau}{\tau}.$$

[1]We found this identity by modifying a standard generating function identity for the Stirling numbers which involved the polylogarithm. It can also be obtained from the formula

$$S(n,k)=\frac{1}{k!}\sum_{i=0}^{k-1}(-1)^i\binom{k}{i}(k-i)^n$$

which can be verified inductively from (4.40).

Authorized licensed use limited to: IEEE Xplore. Downloaded on December 30, 2008 at 06:05 from IEEE Xplore. Restrictions apply.

If $\frac{\tau}{1-\tau} \le e^{1-n}$, then $x_* \le 1$, and so the alternating series

$$F_n(\tau) = \sum_{k=1}^{\infty} (-1)^{n+k} g(k)$$

has magnitude at most $g(1) = \frac{\tau}{1-\tau}$. Otherwise, the series has magnitude at most

$$g(x_*) = e^{(n-1)\left(\log(n-1) - \log\log\frac{1-\tau}{\tau} - 1\right)}$$

and the claim follows. □

Roughly speaking, this means that $F_n(\tau)$ behaves like τ for $n = O(\log[1/\tau])$ and behaves like $(n/\log[1/\tau])^n$ for $n \gg \log[1/\tau]$. In the sequel, it will be convenient to express this bound as

$$F_n(\tau) \le G(n)$$

where

$$G(n) = \begin{cases} \frac{\tau}{1-\tau}, & \log\frac{\tau}{1-\tau} \le 1-n \\ e^{(n-1)\left(\log(n-1) - \log\log\frac{1-\tau}{\tau} - 1\right)}, & \log\frac{\tau}{1-\tau} > 1-n. \end{cases} \tag{4.43}$$

Note that we voluntarily exchanged the function arguments to reflect the idea that we shall view G as a function of n while τ will serve as a parameter.

D. A Second Formula for the Expected Value of the Trace of H_0^{2n}

Let us return to (4.36). The inner sum of (4.36) can be rewritten as

$$\sum_{\sim \in \mathcal{P}(A)} \tau^{|A/\sim|} \sum_{\boldsymbol{\omega} \in \Omega(\sim)} f(\boldsymbol{\omega})$$

with $f(\boldsymbol{\omega}) := e^{\frac{2\pi i}{N} \sum_{1 \le j \le 2n} \omega_j (t_j - t_{j+1})}$. We prove the following useful identity.

Lemma 4.4:

$$\sum_{\sim \in \mathcal{P}(A)} \tau^{|A/\sim|} \sum_{\boldsymbol{\omega} \in \Omega(\sim)} f(\boldsymbol{\omega}) = \sum_{\sim_1 \in \mathcal{P}(A)} \left[\sum_{\boldsymbol{\omega} \in \Omega_{\le}(\sim_1)} f(\boldsymbol{\omega}) \right] \prod_{A' \in A/\sim_1} F_{|A'|}(\tau). \tag{4.44}$$

Proof: Applying (4.37) and rearranging, we may rewrite this as

$$\sum_{\sim_1 \in \mathcal{P}(A)} T(\sim_1) \sum_{\boldsymbol{\omega} \in \Omega_{\le}(\sim_1)} f(\boldsymbol{\omega}),$$

where

$$T(\sim_1) = \sum_{\sim \in \mathcal{P}(A): \sim \ge \sim_1} \tau^{|A/\sim|} (-1)^{|A/\sim| - |A/\sim_1|} \times \prod_{A' \in A/\sim_1} (|A'/\sim| - 1)!.$$

Splitting A into equivalence classes A' of $A/\sim_1$, observe that

$$T(\sim_1) = \prod_{A' \in A/\sim_1} \sum_{\sim' \in \mathcal{P}(A')} \tau^{|A'/\sim'|} (-1)^{|A'/\sim'| - |A'|} (|A'/\sim'| - 1)!;$$

splitting $\sim'$ based on the number of equivalence classes $|A'/\sim'|$, we can write this as

$$\prod_{A' \in A/\sim_1} \sum_{k=1}^{|A'|} S(|A'|, k) \tau^k (-1)^{|A'|-k} (k-1)! = \prod_{A' \in A/\sim_1} F_{|A'|}(\tau)$$

by (4.42). Gathering all this together, we have proven the identity (4.44). □

We specialize (4.44) to the function

$$f(\boldsymbol{\omega}) := e^{\frac{2\pi i}{N} \sum_{1 \le j \le 2n} \omega_j (t_j - t_{j+1})}$$

and obtain

$$\boldsymbol{E}[\mathrm{Tr}(H_0^{2n})] = \sum_{\sim \in \mathcal{P}(A)} \sum_{t_1, \ldots, t_{2n} \in T : t_j \ne t_{j+1}} \times \sum_{\boldsymbol{\omega} \in \Omega_{\le}(\sim)} e^{\frac{2\pi i}{N} \sum_{j=1}^{2n} \omega_j (t_j - t_{j+1})} \prod_{A' \in A/\sim} F_{|A'|}(\tau). \tag{4.45}$$

We now compute

$$I(\sim) = \sum_{\boldsymbol{\omega} \in \Omega_{\le}(\sim)} e^{\frac{2\pi i}{N} \sum_{1 \le j \le 2n} \omega_j (t_j - t_{j+1})}.$$

For every equivalence class $A' \in A/\sim$, let $t_{A'}$ denote the expression $t_{A'} := \sum_{a \in A'} (t_a - t_{a+1})$, and let $\omega_{A'}$ denote the expression $\omega_{A'} := \omega_a$ for any $a \in A'$ (these are all equal since $\boldsymbol{\omega} \in \Omega_{\le}(\sim)$). Then

$$I(\sim) = \sum_{(\omega_{A'})_{A' \in A/\sim} \in \mathbb{Z}_N^{|A/\sim|}} e^{\frac{2\pi i}{N} \sum_{A' \in A/\sim} \omega_{A'} t_{A'}} = \prod_{A' \in A/\sim} \sum_{\omega_{A'} \in \mathbb{Z}_n} e^{\frac{2\pi i}{N} \omega_{A'} t_{A'}}.$$

We now see the importance of (4.45) as the inner sum equals $|\mathbb{Z}_N| = N$ when $t_{A'} = 0$ and vanishes otherwise. Hence, we proved the following.

Lemma 4.5: For every equivalence class $A' \in A/\sim$, let

$$t_{A'} := \sum_{a \in A'} (t_a - t_{a+1}).$$

Then

$$\boldsymbol{E}\left[\mathrm{Tr}\left(H_0^{2n}\right)\right] = \sum_{\sim \in \mathcal{P}(A)} \sum_{t \in T^{2n} : t_j \ne t_{j+1} \text{and } t_{A'} = 0 \text{ for all } A'} N^{|A/\sim|} \prod_{A' \in A/\sim} F_{|A'|}(\tau). \tag{4.46}$$

Authorized licensed use limited to: IEEE Xplore. Downloaded on December 30, 2008 at 06:05 from IEEE Xplore. Restrictions apply.

This formula will serve as a basis for all of our estimates. In particular, because of the constraint $t_j \neq t_{j+1}$, we see that the summand vanishes if $A/\sim$ contains any singleton equivalence classes. This means, in passing, that the only equivalence classes which contribute to the sum obey $|A/\sim| \leq n$.

E. Proof of Theorem 3.3

Let $\sim$ be an equivalence which does not contain any singleton. Then the following inequality holds:

$$\#\left\{t \in T^{2n} : t_{A'} = 0 \text{ for all } A' \in A/\sim\right\} \leq |T|^{2n-|A/\sim|+1}.$$

To see why this is true, observe that as linear combinations of $t_1, \ldots, t_{2n}$, the expressions $t_j - t_{j+1}$ are all linearly independent of each other except for the constraint $\sum_{j=1}^{2n} t_j - t_{j+1} = 0$. Thus, we have $|A/\sim| - 1$ independent constraints in the above sum, and so the number of t's obeying the constraints is bounded by $|T|^{2n-|A/\sim|+1}$.

It then follows from (4.46) and from the bound on the individual terms $F_{|A'|}(\tau)$ (4.43) that

$$\boldsymbol{E}\left(\operatorname{Tr}\left(H_0^{2n}\right)\right) \leq \sum_{k=1}^{n} N^k |T|^{2n-k+1} \sum_{\sim \in \mathcal{P}(A,k)} \prod_{A' \in A/\sim} G(|A'|) \tag{4.47}$$

where $\mathcal{P}(A,k)$ denotes all the equivalence relations on A with k equivalence classes and with no singletons. In other words, the expected value of the trace obeys

$$\boldsymbol{E}\left(\operatorname{Tr}\left(H_0^{2n}\right)\right) \leq \sum_{k=1}^{n} N^k |T|^{2n-k+1} Q(2n,k)$$

where

$$Q(2n,k) := \sum_{\sim \in \mathcal{P}(A,k)} \prod_{A' \in A/\sim} G(|A'|). \tag{4.48}$$

The idea is to estimate the quantity $Q(n,k)$ by obtaining a recursive inequality. Before we do this, however, observe that for $\tau \leq 1/(1+e)$

$$G(n+1) \leq nG(n)$$

for all $n \geq 1$. To see this, we use the fact that $\log G$ is convex and hence,

$$\log G(n+1) \leq \log G(n) + \frac{d}{dn} \log G(n+1).$$

The claim follows by a routine computation which shows that $\frac{d}{dn} \log G(n+1) \leq \log n$ whenever $\log \log \frac{1-\tau}{\tau} \geq 0$.

We now claim the recursive inequality

$$Q(n,k) \leq (n-1)(Q(n-1,k) + G(2)Q(n-2,k-1)) \tag{4.49}$$

which is valid for all $n \geq 3$, $k \geq 1$. To see why this holds, suppose that α is an element of $\{1, \ldots, n\}$ and $\sim$ is in $\mathcal{P}(\{1, \ldots, n\}, k)$. Then either 1) α belongs to an equivalence class that has only one other element β of $\{1, \ldots, n\}$ (for which there are $n-1$ choices), and on taking that class out one obtains the $(n-1)G(2)Q(n-2,k-1)$ term, or 2) α belongs to an equivalence class with more than two elements, thus, removing α from $\{1, \ldots, n\}$ gives rise to an equivalence class in $\mathcal{P}(\{1, \ldots, n\} \backslash \{\alpha\}, k)$. To control this contribution, let $\sim'$ be an element of $\mathcal{P}(\{1, \ldots, n\} \backslash \{\alpha\}, k)$ and let $A_1, \ldots, A_k$ be the corresponding equivalence classes. The element α is attached to one of the classes A_i, and causes $G(|A_i|)$ to increase by at most $|A_i|$. Therefore, this term's contribution is less than

$$\sum_{\sim' \in \mathcal{P}(\{1,\ldots,n\} \backslash \{\alpha\}, k)} \sum_{i=1}^{k} |A_i| \prod_{A' \in \{1,\ldots,n\}/\sim} G(|A'|).$$

But clearly $\sum_{i=1}^{k} |A_i| = n-1$, and so this expression simplifies to $(n-1)Q(n-1,k)$.

From the recursive inequality, one obtains from induction that

$$Q(n,k) \leq G(2)^k (2n)^{n-k}. \tag{4.50}$$

The claim is indeed valid for all $Q(1,k)$'s and $Q(2,k)$'s. Then if one assumes that the claim is established for all pairs (m,k) with $m < n$, the inequality (4.49) shows the property for $m = n$. We omit the details.

The bound (4.50) then automatically yields a bound on the trace

$$\boldsymbol{E}\left(\operatorname{Tr}\left(H_0^{2n}\right)\right) \leq \sum_{k=1}^{n} N^k |T|^{2n-k+1} G(2)^k (4n)^{2n-k}.$$

With $\beta = NG(2)/(4n|T|)$, the right-hand side can be rewritten as $|T|^{2n+1}(4n)^{2n} \sum \beta^k$ and since $\sum \beta^k \leq n \max(\beta, \beta^n)$, we established that

$$\boldsymbol{E}\left(\operatorname{Tr}\left(H_0^{2n}\right)\right) \leq \begin{cases} nN^n |T|^{n+1} G(2)^n (4n)^n, & n \leq \frac{NG(2)}{4|T|} \\ nN|T|^{2n} G(2)(4n)^{2n-1}, & \text{otherwise.} \end{cases}$$

We recall that $G(2) = \tau/(1-\tau)$ and thus, this last inequality is nearly the content of Theorem 3.3 except for the loss of the factor e^n in the case where n is not too large.

To recover this additional factor, we begin by observing that (4.49) gives

$$Q(2k,k) \leq (2k-1)G(2)Q(2(k-1),k-1)$$

since $Q(n,k) = 0$ for $n < 2k$. It follows that

$$Q(2k,k) \leq (2k-1)(2k-3)\ldots 3G(2)^k = \frac{(2k-1)!G(2)^k}{2^{k-1}(k-1)!}$$

and a simple induction shows that

$$\begin{aligned} Q(n,k) &\leq (n-1)(n-2)\ldots 2k 2^{n-k} Q(2k,k) \\ &\leq \frac{(n-1)!}{(k-1)!} 2^{n-2k+1} G(2)^k \end{aligned} \tag{4.51}$$

which is slightly better than (4.50). In short

$$\boldsymbol{E}\left(\operatorname{Tr}\left(H_0^{2n}\right)\right) \leq \sum_{k=1}^{n} B(2n,k)$$

where $B(2n,k) = \frac{(2n-1)!}{(k-1)!} N^k |T|^{2n-k+1} 2^{2n-2k+1} G(2)^k$. One then computes

$$\frac{B(2n,k)}{B(2n,k-1)} = \frac{NG(2)}{4|T|(k-1)}$$

Authorized licensed use limited to: IEEE Xplore. Downloaded on December 30, 2008 at 06:05 from IEEE Xplore. Restrictions apply.

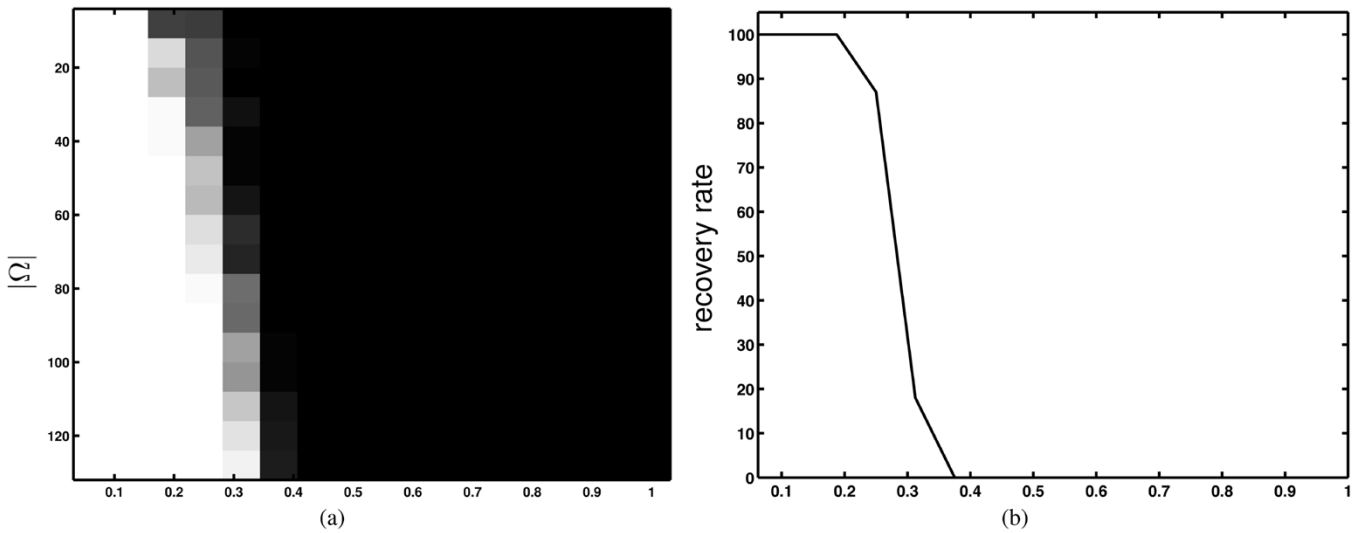

Fig. 2. Recovery experiment for $N = 512$. (a) The image intensity represents the percentage of the time solving (P_1) recovered the signal f exactly as a function of $|\Omega|$ (vertical axis) and $|T|/|\Omega|$ (horizontal axis); in white regions, the signal is recovered approximately 100% of the time, in black regions, the signal is never recovered. For each $|T|, |\Omega|$ pair, 100 experiments were run. (b) Cross section of the image in (a) at $|\Omega| = 64$. We can see that we have perfect recovery with very high probability for $|T| \leq 16$.

and, therefore, for a fixed n obeying $n \leq NG(2)/[4|T|]$, $B(2n,k)$ is nondecreasing with k. Whence

$$\boldsymbol{E}\left(\mathrm{Tr}\left(H_0^{2n}\right)\right) \leq nB(2n,n) = n\frac{2n!}{n!}G(2)^n|T|^{n+1}N^n. \tag{4.52}$$

The ratio $(2n)!/n!$ can be simplified using the classical Stirling approximation

$$\sqrt{2\pi}n^{n+1/2}e^{-n+\frac{1}{12n+1}} < n! < \sqrt{2\pi}n^{n+1/2}e^{-n+\frac{1}{12n}}$$

which gives

$$\frac{2n!}{n!} \leq 2^{2n+1}n^n e^{-n}.$$

The substitution in (4.52) concludes the proof of Theorem 3.3.

V. Numerical Experiments

In this section, we present numerical experiments that suggest empirical bounds on $|T|$ relative to $|\Omega|$ for a signal f supported on T to be the unique minimizer of (P_1). Rather than a rigorous test of Theorem 1.3 (which would be a serious challenge computationally), the results can be viewed as a set of practical guidelines for situations where one can expect perfect recovery from partial Fourier information using convex optimization.

Our experiments are of the following form.

1) Choose constants N (the length of the signal), N_t (the number of spikes in the signal), and N_ω (the number of observed frequencies).
2) Select the subset T uniformly at random by sampling from $\{0,\ldots,N-1\}$ N_t times without replacement (we have $|T| = N_t$).
3) Randomly generate f by setting $f(t) = 0, t \in T^c$, and drawing both the real and imaginary parts of $f(t), t \in T$ from independent Gaussian distributions with mean zero and variance one.[2]
4) Select the subset Ω of observed frequencies of size $|\Omega| = N_\omega$ uniformly at random.
5) Solve (P_1), and compare the solution to f.

To solve (P_1), a very basic gradient descent with projection algorithm was used. Although simple, the algorithm is effective enough to meet our needs here, typically converging in less than 10 s on a standard desktop computer for signals of length $N = 512$. A more refined approach would recast (P_1) as a second-order cone program (or a linear program if f is real), and use a modern interior point solver [6].

Fig. 2 illustrates the recovery rate for varying values of $|T|$ and $|\Omega|$ for $N = 512$. From the plot, we can see that for $|\Omega| \geq 32$, if $|T| \leq |\Omega|/5$, we recover f perfectly about 80% of the time. For $|T| \leq |\Omega|/8$, the recovery rate is practically 100%. We remark that these numerical results are consistent with earlier findings [5], [30].

As pointed out earlier, we would like to reiterate that our numerical experiments are not really "testing" Theorem 1.3 as our experiments concern the situation where both T and Ω are randomly selected while in Theorem 1.3, Ω is random and T can be anything with a fixed cardinality. In other words, extremal or near-extremal signals such as the Dirac comb are unlikely to be observed. To include such signals, one would need to check all subsets T (and there are exponentially many of them), and in accordance with the duality conditions, try all sign combinations on each set T. This distinction between *most* and *all* signals surely explains why there seems to be no logarithmic factor in Fig. 2.

One source of slack in the theoretical analysis is the way in which we choose the polynomial $P(t)$ (as in (2.15)). Theorem 2.1 states that f is a minimizer of (P_1) if and only if there

[2]The results here, as in the rest of the paper, seem to rely only on the sets T and Ω. The actual values that f takes on T can be arbitrary; choosing them to be random emphasizes this. Fig. 2 remain the same if we take $f(t) = 1, t \in T$, say.

Authorized licensed use limited to: IEEE Xplore. Downloaded on December 30, 2008 at 06:05 from IEEE Xplore. Restrictions apply.

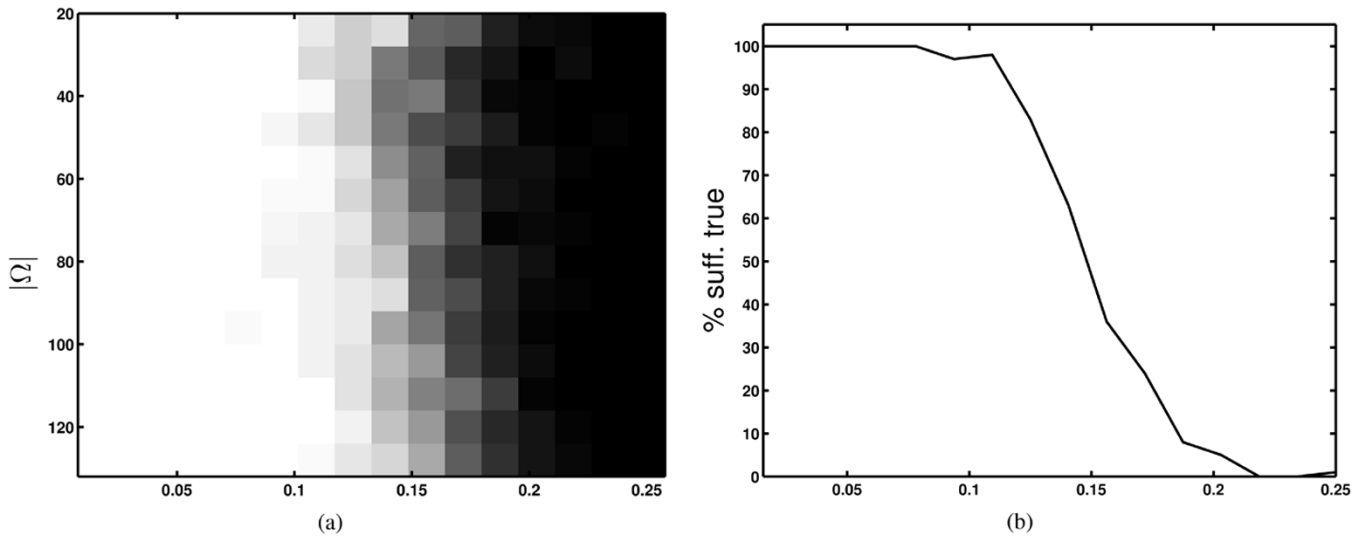

Fig. 3. Sufficient condition test for $N = 512$. (a) The image intensity represents the percentage of the time $P(t)$ chosen as in (2.15) meets the condition $|P(t)| < 1, t \in T^c$. (b) A cross section of the image in (a) at $|\Omega| = 64$. Note that the axes are scaled differently than in Fig. 2.

exists *any* trigonometric polynomial that has $P(t) = \mathrm{sgn}(f)(t)$, $t \in T$, and $|P(t)| < 1$, $t \in T^c$. In (2.15) we choose $P(t)$ that minimizes the ℓ_2 norm on T^c under the linear constraints $P(t) = \mathrm{sgn}(f)(t), t \in T$. (Again, keep in mind here that both T and Ω are randomly chosen.) However, the condition $|P(t)| < 1$ suggests that a minimal ℓ_∞ choice would be more appropriate (but is seemingly intractable analytically).

Fig. 3 illustrates how often the sufficient condition of $P(t)$ chosen as (2.15) meets the constraint $|P(t)| < 1, t \in T^c$ for the same values of τ and $|T|$. The empirical bound on T is stronger by about a factor of two; for $|T| \leq |\Omega|/10$, the success rate is very close to 100%.

As a final example of the effectiveness of this recovery framework, we show two more results of the type presented in Section I-A; piecewise-constant phantoms reconstructed from Fourier samples on a star. The phantoms, along with the minimum energy and minimum total-variation reconstructions (which are exact), are shown in Fig. 4. Note that the total-variation reconstruction is able to recover very subtle image features; for example, both the short and skinny ellipse in the upper right hand corner of Fig. 4(d) and the very faint ellipse in the bottom center are preserved. (We invite the reader to check [1] for related types of experiments.)

VI. Discussion

We would like to close this paper by offering a few comments about the results obtained in this paper and by discussing the possibility of generalizations and extensions.

A. Stability

In the introduction section, we argued that even if one knew the support T of f, the reconstruction might be unstable. Indeed, with knowledge of T, a reasonable strategy might be to recover f by the method of least squares, namely

$$f = (\mathcal{F}^*_{T\to\Omega}\mathcal{F}_{T\to\Omega})^{-1}\mathcal{F}^*_{T\to\Omega}\hat{f}|_\Omega.$$

In practice, the matrix inversion might be problematic. Now observe that with the notations of this paper

$$\mathcal{F}^*_{T\to\Omega}\mathcal{F}_{T\to\Omega} \propto I_T - \frac{1}{|\Omega|}H_0.$$

Hence, for stability we would need $\frac{1}{|\Omega|}H_0 \leq 1 - \delta$ for some $\delta > 0$. This is of course exactly the problem we studied, compare Theorem 3.1. In fact, selecting α_M as suggested in the proof of our main theorem (see Section III-E) gives $\frac{1}{|\Omega|}H_0 \leq 0.42$ with probability at least $1 - O(N^{-M})$. This shows that selecting $|T|$ as to obey (1.6), $|T| \approx |\Omega|/\log N$ actually provides stability.

B. Robustness

An important question concerns the robustness of the reconstruction procedure vis a vis measurement errors. For example, we might want to consider the model problem which says that instead of observing the Fourier coefficients of f, one is given those of $f + h$ where h is some small perturbation. Then one might still want to reconstruct f via

$$f^\sharp = \arg\min\|g\|_{\ell_1}, \quad \hat{g}(\omega) = \hat{f}(\omega) + \hat{h}(\omega), \quad \forall\, \omega \in \Omega.$$

In this setup, one cannot expect exact recovery. Instead, one would like to know whether or not our reconstruction strategy is well behaved or more precisely, how far is the minimizer $f^\sharp$ from the true object f. In short, what is the typical size of the error? Our preliminary calculations suggest that the reconstruction is robust in the sense that the error $\|f - f^\sharp\|_1$ is small for small perturbations h obeying $\|h\|_1 \leq \delta$, say. We hope to be able to report on these early findings in a follow-up paper.

C. Extensions

Finally, work in progress shows that similar exact reconstruction phenomena hold for other synthesis/measurement pairs. Suppose one is given a pair of bases $(\mathcal{B}_1, \mathcal{B}_2)$ and randomly selected coefficients of an object f in one basis, say $\mathcal{B}_2$. (From this broader viewpoint, the special cases discussed in this paper assume that $\mathcal{B}_1$ is the canonical basis of $\mathbb{R}^N$ or $\mathbb{R}^N \times \mathbb{R}^N$ (spikes

Authorized licensed use limited to: IEEE Xplore. Downloaded on December 30, 2008 at 06:05 from IEEE Xplore. Restrictions apply.

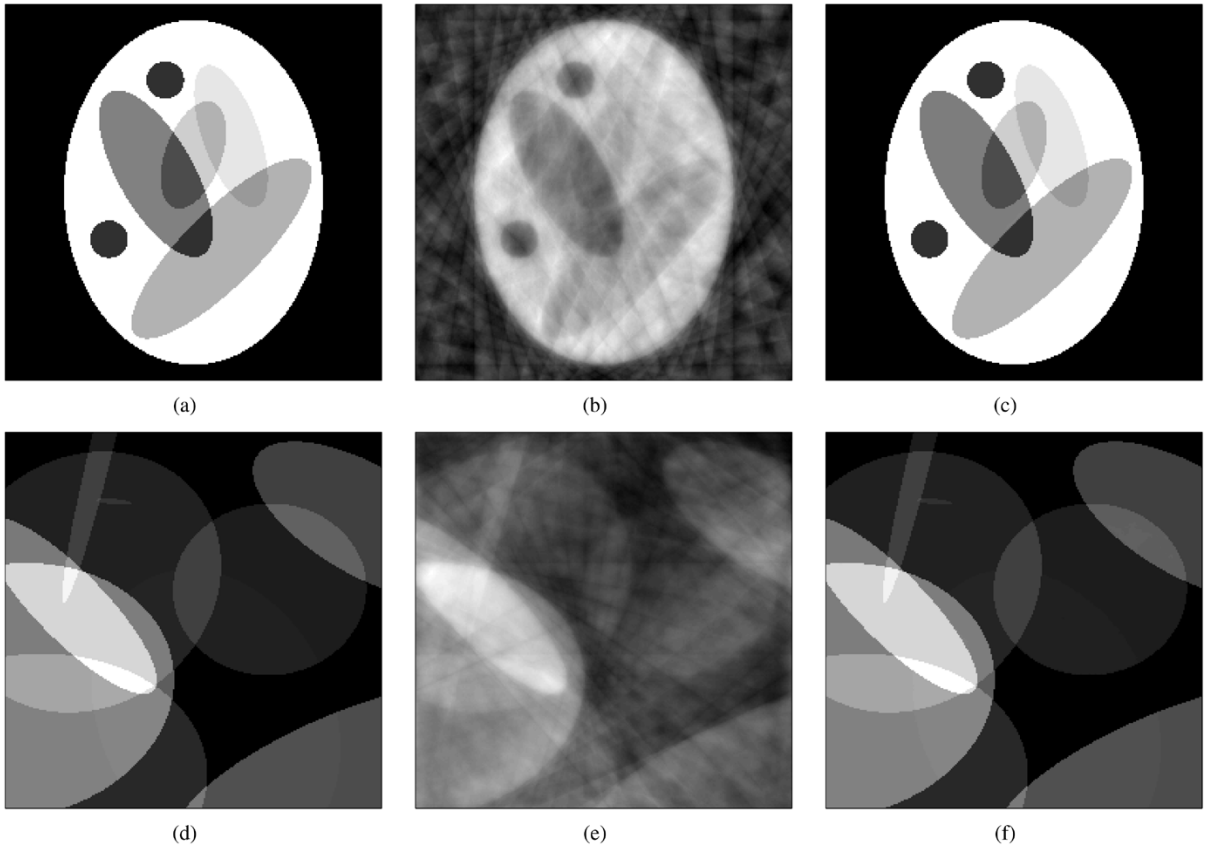

Fig. 4. Two more phantom examples for the recovery problem discussed in Section I-A. On the left is the original phantom ((d) was created by drawing ten ellipses at random), in the center is the minimum energy reconstruction, and on the right is the minimum total-variation reconstruction. The minimum total-variation reconstructions are exact.

in 1D, 2D), or is the basis of Heavisides as in the total-variation reconstructions, and $\mathcal{B}_2$ is the standard 1D, 2D Fourier basis.) Then, it seems that f can be recovered exactly provided that it may be synthesized as a sparse superposition of elements in $\mathcal{B}_1$. The relationship between the number of nonzero terms in $\mathcal{B}_1$ and the number of observed coefficients depends upon the *incoherence* between the two bases [5]. The more incoherent, the fewer coefficients needed. Again, we hope to report on such extensions in a separate publication.

APPENDIX

A. Proof of Lemma 2.1

We may assume that Ω is nonempty and that f is nonzero since the claims are trivial otherwise.

Suppose first that such a function P exists. Let g be any vector not equal to f with $\hat{g}|_\Omega = \hat{f}|_\Omega$. Write $h := g - f$, then $\hat{h}$ vanishes on Ω. Observe that for any $t \in T$ we have

$$\begin{aligned} |g(t)| &= |f(t) + h(t)| \\ &= |f(t)| + h(t)\overline{\mathrm{sgn}(f)(t)}| \\ &\geq |f(t)| + \mathrm{Re}(h(t)\overline{\mathrm{sgn}(f)(t)}) \\ &= |f(t)| + \mathrm{Re}(h(t)\overline{P(t)}) \end{aligned}$$

while for $t \notin T$ we have

$$|g(t)| = |h(t)| \geq \mathrm{Re}(h(t)\overline{P(t)})$$

since $|P(t)| < 1$. Thus,

$$||g||_{\ell_1} \geq ||f||_{\ell_1} + \sum_{t=0}^{N-1} \mathrm{Re}(h(t)\overline{P(t)}).$$

However, the Parseval's formula gives

$$\sum_{t=0}^{N-1} \mathrm{Re}(h(t)\overline{P(t)}) = \frac{1}{N} \sum_{k=0}^{N-1} \mathrm{Re}(\hat{h}(k)\overline{\hat{P}(k)}) = 0$$

since $\hat{P}$ is supported on Ω and $\hat{h}$ vanishes on Ω. Thus, $||g||_{\ell_1} \geq ||f||_{\ell_1}$. Now we check when equality can hold, i.e., when $||g||_{\ell_1} = ||f||_{\ell_1}$. An inspection of the above argument shows that this forces $|h(t)| = \mathrm{Re}(h(t)\overline{P(t)})$ for all $t \notin T$. Since $|P(t)| < 1$, this forces h to vanish outside of T. Since $\hat{h}$ vanishes on Ω, we thus see that h must vanish identically (this follows from the assumption about the injectivity of $\mathcal{F}_{T\to\Omega}$) and so $g = f$. This shows that f is the unique minimizer $f^\sharp$ to the problem (1.5).

Conversely, suppose that $f = f^\sharp$ is the unique minimizer to (1.5). Without loss of generality, we may normalize $||f||_{\ell_1} = 1$. Then the closed unit ball $B := \{g : ||g||_{\ell_1} \leq 1\}$ and the affine space $V := \{g : \hat{g}|_\Omega = \hat{f}|_\Omega\}$ intersect at exactly one point, namely, f. By the Hahn–Banach theorem we can thus find a function P such that the hyperplane

$$\Gamma_1 := \left\{ g : \sum \mathrm{Re}(g(t)\overline{P(t)}) = 1 \right\}$$

Authorized licensed use limited to: IEEE Xplore. Downloaded on December 30, 2008 at 06:05 from IEEE Xplore. Restrictions apply.

contains V, and such that the half space

$$\Gamma_{\leq 1} := \{g : \sum \mathrm{Re}(g(t)\overline{P(t)}) \leq 1\}$$

contains B. By perturbing the hyperplane if necessary (and using the uniqueness of the intersection of B with V) we may assume that $\Gamma_1 \cap B$ is contained in the minimal facet of B which contains f, namely, $\{g \in B : \mathrm{supp}(g) \subseteq T\}$.

Since B lies in $\Gamma_{\leq 1}$, we see that $\sup_t |P(t)| \leq 1$; since $f \in \Gamma_1 \cap B$, we have $P(t) = \mathrm{sgn}(f)(t)$ when $t \in \mathrm{supp}(f)$. Since $\Gamma_1 \cap B$ is contained in the minimal facet of B containing f, we see that $|P(t)| < 1$ when $t \notin T$. Since Γ_1 contains V, we see from Parseval that $\hat{P}$ is supported in Ω. The claim follows.

B. Proof of Lemma 3.4

Set $e^{i\phi} = \mathrm{sgn}(f)$ for short, and fix K. Using (3.19), we have

$$[(H\iota^*)^{n+1}e^{i\phi}](t_0) = \sum_{t_1,\ldots,t_{n+1}\in T : t_j \neq t_{j+1} \text{ for } j=0,\ldots,n} \; \sum_{\omega_0,\ldots,\omega_n \in \Omega} e^{\frac{2\pi i}{N}\sum_{j=0}^{n}\omega_j(t_j - t_{j+1})} e^{i\phi(t_{n+1})}$$

and, for example,

$$\begin{aligned}|[(H\iota^*)^{n+1}e^{i\phi}](t_0)|^2 &= \sum_{\substack{t_1,\ldots,t_{n+1}\in T : t_j \neq t_{j+1} \text{ for } j=0,\ldots,n \\ t'_1,\ldots,t'_{n+1}\in T : t'_j \neq t'_{j+1} \text{ for } j=0,\ldots,n}} e^{i\phi(t_{n+1})}e^{-i\phi(t'_{n+1})} \\ &\quad \times \sum_{\substack{\omega_0,\ldots,\omega_n\in\Omega \\ \omega'_0,\ldots,\omega'_n\in\Omega}} e^{\frac{2\pi i}{N}\sum_{j=0}^{n}\omega_j(t_j - t_{j+1})} \\ &\quad \times e^{-\frac{2\pi i}{N}\sum_{j=0}^{n}\omega'_j(t'_j - t'_{j+1})}.\end{aligned}$$

One can calculate the $2K$th moment in a similar fashion. Put $m := K(n+1)$ and

$$\boldsymbol{\omega} := \left(\omega_j^{(k)}\right)_{k,j}, \quad \boldsymbol{t} = \left(t_j^{(k)}\right)_{k,j} \in T^{2K(n+1)}$$

for $1 \leq j \leq n+1$ and $1 \leq k \leq 2K$. With these notations, we have

$$|[(H\iota^*)^{n+1}g](t_0)|^{2K} = \sum_{\boldsymbol{t}\in T^{2m} : t_j^{(k)} \neq t_{j+1}^{(k)}} \; \sum_{\boldsymbol{\omega}\in\Omega^{2m}} e^{i\sum_{k=1}^{2K}(-1)^k\phi\left(t_{n+1}^{(k)}\right)} e^{\frac{2\pi i}{N}\sum_{k=1}^{2K}\sum_{j=0}^{n}(-1)^k\omega_j^{(k)}(t_j^{(k)} - t_{j+1}^{(k)})}$$

where we adopted the convention that $x_0^{(k)} = x_0$ for all $1 \leq k \leq 2K$ and where it is understood that the condition $t_j^{(k)} \neq t_{j+1}^{(k)}$ is valid for $0 \leq j \leq n$.

Now the calculation of the expectation goes exactly as in Section IV. Indeed, we define an equivalence relation $\sim_{\boldsymbol{\omega}}$ on the finite set $A := \{0,\ldots,n\} \times \{1,\ldots,2K\}$ by setting $(j,k) \sim (j',k')$ if $\omega_j^{(k)} = \omega_{j'}^{(k')}$ and observe as before that

$$\boldsymbol{E}\left[\prod_{j,k} I_{\omega_j^{(k)}}\right] = \tau^{|A/\sim|};$$

that is, τ raised at the power that equals the number of distinct ω's and, therefore, we can write the expected value $m(n;K)$ as

$$m(n;K) = \sum_{\boldsymbol{t}\in T^{2m} : t_j^{(k)} \neq t_{j+1}^{(k)}} e^{i\sum_{k=1}^{2K}(-1)^k\phi(t_{n+1}^{(k)})} \sum_{\sim\in\mathcal{P}(A)} \tau^{|A/\sim|} \times \sum_{\boldsymbol{\omega}\in\Omega^{(\sim)}} e^{\frac{2\pi i}{N}\sum_{k=1}^{2K}\sum_{j=0}^{n}(-1)^k\omega_j^{(k)}\left(t_j^{(k)} - t_{j+1}^{(k)}\right)}.$$

As before, we follow Lemma 4.5 and rearrange this as

$$m(n;K) = \sum_{\sim\in\mathcal{P}(A)} \sum_{\boldsymbol{t}\in T^{2m} : t_j^{(k)} \neq t_{j+1}^{(k)}} e^{i\sum_{k=1}^{2K}(-1)^k\phi\left(t_{n+1}^{(k)}\right)} \times \prod_{A'\in A/\sim} F_{|A'|}(\tau) \times \sum_{\boldsymbol{\omega}\in\Omega^{(\sim)}} e^{\frac{2\pi i}{N}\sum_{k=1}^{2K}\sum_{j=0}^{n}(-1)^k\omega_j^{(k)}\left(t_j^{(k)} - t_{j+1}^{(k)}\right)}.$$

As before, the summation over $\boldsymbol{\omega}$ will vanish unless

$$t_{A'} := \sum_{(j,k)\in A'} (-1)^k(t_j^{(k)} - t_{j+1}^{(k)}) = 0$$

for all equivalence classes $A' \in A/\sim$, in which case the sum equals $N^{|A/\sim|}$. In particular, if $A/\sim$, the sum vanishes because of the constraint $t_j^{(k)} \neq t_{j+1}^{(k)}$, so we may just as well restrict the summation to those equivalence classes that contain no singletons. In particular, we have

$$|A/\sim| \leq K(n+1) = m. \tag{7.53}$$

To summarize

$$\begin{aligned}m(n,K) &= \sum_{\sim\in\mathcal{P}(A)} \sum_{\boldsymbol{t}\in T^{2m} : t_j^{(k)} \neq t_{j+1}^{(k)} \text{ and } t_{A'}=0 \text{ for all } A'} \\ &\quad \times e^{i\sum_{k=1}^{2K}(-1)^k\phi\left(t_{n+1}^{(k)}\right)} N^{|A/\sim|} \prod_{A'\in A/\sim} F_{|A'|}(\tau) \\ &\leq \sum_{\sim\in\mathcal{P}(A)} \sum_{\boldsymbol{t}\in T^{2K(n+1)} : t_j^{(k)} \neq t_{j+1}^{(k)} \text{ and } t_{A'}=0 \text{ for all } A'} \\ &\quad \times N^{|A/\sim|} \prod_{A'\in A/\sim} F_{|A'|}(\tau),\end{aligned} \tag{7.54}$$

since

$$|e^{i\sum_{k=1}^{2K}(-1)^k\phi(t_{n+1}^{(k)})}| = 1.$$

Observe the striking resemblance with (4.46). Let $\sim$ be an equivalence which does not contain any singleton. Then the following inequality holds:

$$\#\{\boldsymbol{t}\in T^{2K(n+1)} : t_{A'}=0, \forall\, A' \in A/\sim\} \leq |T|^{2K(n+1)-|A/\sim|}.$$

To see why this is true, observe as linear combinations of the $t_j^{(k)}$ and of t_0, we see that the expressions $t_j^{(k)} - t_{j+1}^{(k)}$ are all linearly independent, and hence the expressions

$$\sum_{(j,k)\in A} (-1)^k(t_j^{(k)} - t_{j+1}^{(k)})$$

Authorized licensed use limited to: IEEE Xplore. Downloaded on December 30, 2008 at 06:05 from IEEE Xplore. Restrictions apply.

are also linearly independent. Thus, we have $|A/\sim|$ independent constraints in the above sum, and so the number of t's obeying the constraints is bounded by $|T|^{2K(n+1)-|A/\sim|}$.

With the notations of Section IV, we established

$$m(n,K) \le \sum_{k=1}^{m} N^k |T|^{2m-k} \sum_{\sim \in \mathcal{P}(A,k)} \prod_{A' \in A/\sim} G(|A'|). \tag{7.55}$$

Now this is exactly the same as (4.47) which we proved obeys the desired bound.

ACKNOWLEDGMENT

E. J. Candes and T. Tao wish to thank the Institute for Pure and Applied Mathematics at the University of California at Los Angeles (UCLA) for their warm hospitality. E. J. Candes would also like to thank Amos Ron and David Donoho for stimulating conversations, and Po-Shen Loh for early numerical experiments on a related project. We would also like to thank Holger Rauhut for corrections on an earlier version and the anonymous referees for their comments and references.

REFERENCES

[1] A. H. Delaney and Y. Bresler, "A fast and accurate iterative reconstruction algorithm for parallel-beam tomography," *IEEE Trans. Image Process.*, vol. 5, no. 5, pp. 740–753, May 1996.

[2] C. Mistretta, private communication, 2004.

[3] T. Tao, "An uncertainty principle for cyclic groups of prime order," *Math. Res. Lett.*, vol. 12, no. 1, pp. 121–127, 2005.

[4] D. L. Donoho and P. B. Stark, "Uncertainty principles and signal recovery," *SIAM J. Appl. Math.*, vol. 49, no. 3, pp. 906–931, 1989.

[5] D. L. Donoho and X. Huo, "Uncertainty principles and ideal atomic decomposition," *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 2845–2862, Nov. 2001.

[6] J. Nocedal and S. J. Wright, *Numerical Optimization*, ser. Springer Series in Operations Research. New York: Springer-Verlag, 1999.

[7] D. L. Donoho and B. F. Logan, "Signal recovery and the large sieve," *SIAM J. Appl. Math.*, vol. 52, no. 2, pp. 577–591, 1992.

[8] D. C. Dobson and F. Santosa, "Recovery of blocky images from noisy and blurred data," *SIAM J. Appl. Math.*, vol. 56, no. 4, pp. 1181–1198, 1996.

[9] F. Santosa and W. W. Symes, "Linear inversion of band-limited reflection seismograms," *SIAM J. Sci. Statist. Comput.*, vol. 7, no. 4, pp. 1307–1330, 1986.

[10] S. S. Chen, D. L. Donoho, and M. A. Saunders, "Atomic decomposition by basis pursuit," *SIAM J. Sci. Comput.*, vol. 20, no. 1, pp. 33–61, 1998.

[11] D. W. Oldenburg, T. Scheuer, and S. Levy, "Recovery of the acoustic impedance from reflection seismograms," *Geophys.*, vol. 48, pp. 1318–1337, 1983.

[12] S. Levy and P. K. Fullagar, "Reconstruction of a sparse spike train from a portion of its spectrum and application to high-resolution deconvolution," *Geophys.*, vol. 46, pp. 1235–1243, 1981.

[13] D. L. Donoho and M. Elad, "Optimally sparse representation in general (nonorthogonal) dictionaries via ℓ_1 minimization," *Proc. Nat. Acad. Sci. USA*, vol. 100, no. 5, pp. 2197–2202 , 2003.

[14] M. Elad and A. M. Bruckstein, "A generalized uncertainty principle and sparse representation in pairs of bases," *IEEE Trans. Inf. Theory*, vol. 48, no. 9, pp. 2558–2567, Sep. 2002.

[15] A. Feuer and A. Nemirovski, "On sparse representation in pairs of bases," *IEEE Trans. Inf. Theory*, vol. 49, no. 6, pp. 1579–1581, Jun. 2003.

[16] R. Gribonval and M. Nielsen, "Sparse representations in unions of bases," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3320–3325, Dec. 2003.

[17] J. A. Tropp, "Greed is good: Algorithmic results for sparse approximation," *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2231–2242, Oct. 2004.

[18] ——, "Just relax: Convex programming methods for subset selection and sparse approximation," *IEEE Trans. Inf. Theory*, submitted for publication.

[19] P. Feng and Y. Bresler, "Spectrum-blind minimum-rate sampling and reconstruction of multiband signals," in *Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing*, vol. 2, Atlanta, GA, 1996, pp. 1689–1692.

[20] P. Feng, S. Yau, and Y. Bresler, "A multicoset sampling approach to the missing cone problem in computer aided tomography," in *Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing*, vol. 2, Atlanta, GA, 1996, pp. 734–737.

[21] M. Vetterli, P. Marziliano, and T. Blu, "Sampling signals with finite rate of innovation," *IEEE Trans. Signal Process.*, vol. 50, no. 6, pp. 1417–1428, Jun. 2002.

[22] A. C. Gilbert, S. Guha, P. Indyk, S. Muthukrishnan, and M. J. Strauss, "Near-optimal sparse fourier representations via sampling," in *Proc. 34th ACM Symp. Theory of Computing*, Montreal, QC, Canada, May 2002, pp. 152–161.

[23] A. C. Gilbert, S. Muthukrishnan, and M. J. Strauss, "Beating the B^2 Bottleneck in Estimating B-Term Fourier Representations," unpublished manuscript, May 2004.

[24] J.-J. Fuchs, "On sparse representations in arbitrary redundant bases," *IEEE Trans. Inf. Theory*, vol. 50, no. 6, pp. 1341–1344, Jun. 2004.

[25] K. Jogdeo and S. M. Samuels, "Monotone convergence of binomial probabilities and a generalization of Ramanujan's equation," *Ann. Math. Statist.*, vol. 39, pp. 1191–1195, 1968.

[26] S. Boucheron, G. Lugosi, and P. Massart, "A sharp concentration inequality with applications," *Random Structures Algorithms*, vol. 16, no. 3, pp. 277–292, 2000.

[27] H. J. Landau and H. O. Pollak, "Prolate spheroidal wave functions, Fourier analysis and uncertainty. II," *Bell Syst. Tech. J.*, vol. 40, pp. 65–84, 1961.

[28] H. J. Landau, "The eigenvalue behavior of certain convolution equations," *Trans. Amer. Math. Soc.*, vol. 115, pp. 242–256, 1965.

[29] H. J. Landau and H. Widom, "Eigenvalue distribution of time and frequency limiting," *J. Math. Anal. Appl.*, vol. 77, no. 2, pp. 469–481, 1980.

[30] E. J. Candes and P. S. Loh, "Image Reconstruction With Ridgelets," Calif. Inst. Technology, SURF Tech. Rep., 2002.

[31] L. I. Rudin, S. Osher, and E. Fatemi, "Nonlinear total variation noise removal algorithm," *Physica D.*, vol. 60, no. 1–4, pp. 259–268, 1992.

Authorized licensed use limited to: IEEE Xplore. Downloaded on December 30, 2008 at 06:05 from IEEE Xplore. Restrictions apply.