DIMACS Technical Report 2001-44
November 2001

Near-Optimal Sparse Fourier Representations via Sampling

by

Anna C. Gilbert[1] Sudipto Guha [2] Piotr Indyk [3] S. Muthukrishnan[1]
Martin J. Strauss[1]

[1]AT&T Labs—Research, 180 Park Avenue, Florham Park, NJ 07932 USA, {agilbert, muthu, mstrauss}@research.att.com, Permanent Members of DIMACS
[2]Department of Computer and Information Science, University of Pennsylvania, Philadelphia, PA 19104, sudipto@cis.upenn.edu
[3]MIT Laboratory for Computer Science; 545 Technology Square, NE43-373; Cambridge, Massachusetts 02139-3594; indyk@theory.lcs.mit.edu

---

DIMACS is a partnership of Rutgers University, Princeton University, AT&T Labs-Research, Bell Labs, NEC Research Institute and Telcordia Technologies (formerly Bellcore).

DIMACS was founded as an NSF Science and Technology Center, and also receives support from the New Jersey Commission on Science and Technology.

ABSTRACT

We give an algorithm for finding a Fourier representation $\mathbf{r}$ of B terms for a given discrete signal $\mathbf{a}$ of length N, such that $\|\mathbf{a} - \mathbf{r}\|_2^2$ is within the factor $(1 + \epsilon)$ of best possible $\|\mathbf{a} - \mathbf{r}_{\text{opt}}\|_2^2$. Our algorithm can access $\mathbf{a}$ by reading its values on a sample set $T \subseteq [0, N)$, chosen randomly from a (non-product) distribution of our choice, independent of $\mathbf{a}$. That is, we sample non-adaptively. The total time cost of the algorithm is polynomial in $B \log(N) \log(M)/\epsilon$ (where M is a standard input precision parameter), which implies a similar bound for the number of samples.

1 Introduction

A Fourier series decomposes a signal into its trigonometric components, which vibrate at various frequencies. Formally, let $\mathbf{a} = (a(0), \ldots, a(N-1))$ be a discrete signal of length N. We let $\psi_\omega(t)$ denote the ω'th Fourier basis function $\frac{1}{\sqrt{N}} e^{2\pi i \omega t/N}$. Then $\hat{a}(\omega) = \frac{1}{\sqrt{N}} \sum_t a(t) e^{-2\pi i \omega t/N}$ is the ω'th Fourier coefficient of $\mathbf{a}$. Fourier analysis, which consists of studying the Fourier coefficients of functions, is textbook material by now; it is a prolific area of mathematical research by itself, with applications to lossy compression, signal and speech processing, fast computation of convolutions, solving partial differential equations, and others too numerous to list. The Fast Fourier Transform that computes *all* the N Fourier coefficients in $O(N \log N)$ operations is a cornerstone: it is used for computing convolutions and elsewhere in computational algebra. Often, however, Fourier analysis involves filtering out noise (the Fourier coefficients corresponding to unwanted frequencies can be eliminated) or detecting the signal (Fourier coefficients that are smaller—in absolute value—than some specified tolerance can be discarded). This filtering is done because the large coefficients capture the major time-invariant wave-like features of the signal. The large coefficients are useful in data compression, feature extraction, finding approximate periods and other data mining tasks. Thus the problem of finding a small set of the largest Fourier coefficients of a signal that capture most of the signal trends is a fundamental task in Fourier analysis and its applications. We address the question of how these coefficients can be estimated fast and accurately.

Suppose we are given an upper bound M on $\|\mathbf{a}\|_2$. Our *main result* in this paper is an algorithm that samples at most $\mathrm{poly}(B \log(N) \log(M)/\epsilon)$ positions of the signal and outputs a Fourier representation $\mathbf{r}$ of B terms such that $\|\mathbf{a} - \mathbf{r}\|_2^2$ is within the factor $(1+\epsilon)$ of best possible $\|\mathbf{a} - \mathbf{r}_{\mathrm{opt}}\|_2^2$. In fact, the sampled positions are independent of the signal. The total computation time is also $\mathrm{poly}(B \log(N) \log(M)/\epsilon)$. Even though the number of sampled positions is significantly sublinear in N (polylogarithmic in various parameters), the outcome is nearly the best choice of B Fourier coefficients. This is the first known result that accurately estimates Fourier representations compactly (in polylogarithmic "space" or samples) and rapidly (in polylogarithmic time without even having to read the entire input—this is possible because the basis functions have wide support). Our result is intriguing. After all, no algorithm can even estimate the *average* of the signal values, or, therefore, any nontrivial norm in similar bounds using $o(N)$ samples. In particular, no algorithm can estimate $\|\mathbf{a}\|_2$ accurately within the sampling complexity above. This in turn means we can not estimate $\|\mathbf{a} - \mathbf{r}\|_2^2$, the quality of our output representation. Nevertheless, our analysis proves that our algorithm based on samples is provably accurate to $1 + \epsilon$ in providing the best B Fourier coefficient representation of a signal. We expect our algorithm to find many uses in computational Fourier analysis.

Mathematically speaking, we are recovering a signal from sample values of that function but using a particular type of signal recovery. We ask to recover $\mathbf{a}$ from the class of B-term trigonometric polynomials. This recovery $\mathbf{r}$ is not the optimal representation $\mathbf{r}_{\mathrm{opt}}$ from among all possible but we can guarantee that if the optimal ℓ^2 error is $\delta \neq 0$, then the error of our recovery is within a factor $(1+\epsilon)$; *i.e.*, $\|\mathbf{a} - \mathbf{r}\|_2^2 \leq (1+\epsilon)\delta$. (Up to precision issues, we recover $\mathbf{a}$ exactly if $\mathbf{a}$ consists exactly of B frequencies.) Our work is related to mathematical ideas that have been around for decades, as well as recent works in theoretical computer science. In what follows, we will place our work in the context of topics from signal processing, mathematical uncertainty principles and learning theory, among other areas.

Signal Processing. There are many signal processing results pertaining to signal recovery from "sampled" values of a function. We restrict ourselves to the "classical" result: the Shannon sampling theorem [10]. It says that you can exactly reconstruct a continuous-time function $\mathbf{f}$ from its sampled values, provided the nonzero Fourier coefficients all lie within the interval $[-\pi/T, \pi/T]$ and the samples are taken at regular spaced points in time, each separated by T. If the largest frequency $\mathbf{f}$ contains is $1/2T$, then we are sampling $\mathbf{f}$ at the Nyquist frequency (and hence fewer samples would be insufficient to reconstruct $\mathbf{f}$ exactly). The reconstruction procedure in the Shannon sampling theorem is very different from our setting. The representation is a linear combination of translates of one basis function with sample values as weights and it is exact, as opposed to approximate reconstruction using trigonometric polynomials that we do here. There are many other interpolation and/or signal recovery algorithms that use sample values or simple functions of sample values as coefficients in a linear reconstruction procedure with different building block functions.

Mathematics and Classical Uncertainty Principles. Let $\mathbf{a}$ be a sequence of length N and let $\hat{\mathbf{a}}$ be its discrete Fourier transform. Let N_t and $N_w = B$ be the number of nonzero values in $\mathbf{a}$ and $\hat{\mathbf{a}}$ respectively. The discrete time uncertainty principle says

Theorem 1 *(Donoho and Stark [3]) For all* $\mathbf{a}$*,* $N_t N_w \geq \Omega(N)$.

This implies that any approximation to a signal cannot be simultaneously sparse in both time and frequency. Thus we cannot hope to construct a representation for $\mathbf{a}$ that consists of B frequencies and B spikes if $B^2 < N$. This is in contrast to other types of representations (*e.g.*, histograms and singular value decompositions), in which one can produce compact representations that are sparse in time as well.

Algorithmic Version of Uncertainty Principle. Suppose that we wish to reconstruct a signal $\mathbf{a}$ but we observe $\mathbf{a}(t)$ only on some index set T. In addition, we know that $\mathbf{a}$ is synthesized using only B frequencies. The (contrapositive of) uncertainty principle tells us [3]:

> For all B and *all* sample sets T, if $\mathbf{a}$ has only B frequencies and $|T| \geq N - O(N/B)$, then $\mathbf{a}$ can be reconstructed from samples on T.

This result is tight over the entire range of $|T|$ and B—for any B that divides N, there are two different functions, each limited to B frequencies, that agree on some T of size just less than $(N - N/B)$—these functions cannot be distinguished. By contrast, one of our results says (where each sample in T is chosen uniformly and independently from $[0, N)$ and $\tilde{\Omega}$ suppresses factors of $\log(N)$ and $\log B$),

> For all B and *most* sample sets T, if $\mathbf{a}$ has only B frequencies and $|T| \geq \tilde{\Omega}(B)$, then $\mathbf{a}$ can be reconstructed from samples on T.

In some applications, the sample set T is adversarially forced. When T can be chosen even randomly, however, and $B \ll N$, our results give reconstruction from a sample set of size perhaps exponentially smaller than what is guaranteed by the uncertainty principle. Thus our results here imply that the uncertainty bound is loose in this context, which may be of independent interest.

The preceding discussion of the context of our work concerns only the number of samples needed to reconstruct $\mathbf{a}$, and applies even when the reconstruction time is $\Omega(N)$. We note that a

significant contribution of our work is bounding the *time* to construct a representation. (Indeed, in order to bound the reconstruction time, our algorithm uses a sample set T that is larger then above and drawn from a distribution more complicated than the uniform distribution.) Thus we regard our work as a (computational) time-bounded strengthening of the uncertainty principle.

Theoretical Computer Science. There are three threads that apply, and we will distinguish our work on all three counts.

First, a relationship was established in [8] between Fourier spectra and learnability. For the class of Boolean functions, the discrete Boolean Fourier basis was defined based on the parity of subsets of the input variables. This representation was used to demonstrate learnability of functions. In [7], authors presented a polynomial time algorithm to find all the large coefficients for this Fourier basis for given Boolean functions. Our work here is related to [7]. Clearly their Fourier basis is different from ours (parity of subsets vs trigonometric polynomials). Our basis is the classical one used in convolutions and other well-known applications, while the one in [8, 7] proves useful in learning theory context (see [9] for a nice overview of the relationship between their Fourier transforms and complexity theory). Our technique is related to [7] at the high level involving the test of groups of coefficients in order to isolate the large ones, but the technical details are vastly different.

Second, there has been recent work on approximating matrices by low rank ones. In particular, in [4], the authors find a matrix D^* from a given matrix A in time polynomial in k such that $\|A-D^*\|_F \leq \max_{\mathrm{rank}(D)\leq k} \|A-D\|_F+\epsilon\|A\|_F$; here $\|\cdot\|_F$ is the Frobenius norm which is the sum of the squares of matrix entries. This work is related to ours since the authors find the k significant singular values; however, the two contexts and techniques are very different. In particular, their work involves weighted sampling of entries in A which can be implemented by scanning A once in linear time. They do not face the challenge of estimating norms or inner products or group testing to find the largest coefficients as we do here. See [1] for further work, but no direct relevance to our work exists.

Finally, our work here is related to our earlier work on finding B significant wavelet coefficients or B-bucket histograms that are piecewise constant representation of the signal. Both seek a $(1+\epsilon)$ approximation to the best size-B representation (B histogram buckets, B wavelet terms, or B Fourier terms). Both use the same high-level strategy: Identify big basis functions by randomized group testing, estimate coefficient values, and subtract from the residual under an overall classic greedy pursuit algorithm. However, there the results themselves differ greatly on most technical issues. The algorithm of [5] works in the streaming model and looks at the entire signal as it necessarily must because sampling will not provide the result there as the basis functions have narrow support. It uses very large-support randomized linear projections a la Johnson and Lindenstrauss [6]. By contrast, we use only samples. The main obstacle in this paper is that we cannot even reliably estimate norms by sampling; by contrast, in [5] norm estimation is easy. As a result, our work here requires significantly different technical machinery as will be evident from the rest of this paper.

Organization. The paper is organized as follows. In Section 3, we give an ideal version of our algorithm, that is infeasible in the sampling model. We thereby give the overall structure of the algorithm that we later introduce and we give names for the various parts. In Section 4, we revisit each element of the ideal algorithm, modifying it if necessary, then implementing it in the

sampling model. In Section 5, we show how to estimate $\|\mathbf{a}-\mathbf{r}\|_2^2$, given $\|\mathbf{a}\|_2^2$ by oracle. Some variants of the algorithm are given in Appendix A. In this extended abstract, all proofs are deferred to Appendix B.

2 Notation and Preliminaries

Let $\mathbf{a} = (a(0), \ldots, a(N-1))$ be a signal indexed by t, regarded as an integer mod N. We denote by $\psi_\omega(t)$ the ω'th Fourier basis function $\frac{1}{\sqrt{N}} e^{2\pi i \omega t/N}$. Then $\hat{a}(\omega) = \langle \mathbf{a}, \psi_\omega \rangle = \frac{1}{\sqrt{N}} \sum_t a(t) e^{-2\pi i \omega t/N}$ is the ω'th Fourier coefficient of $\mathbf{a}$. (Note that $\langle \mathbf{a}, \mathbf{b} \rangle = \sum_t a(t)\overline{b(t)}$, where $\overline{b(t)}$ is the complex conjugate of $b(t)$.) The vector $\hat{\mathbf{a}}$ is the *spectrum* of $\mathbf{a}$. The basis functions in the time domain are denoted δ_t, so $\delta_t(s)$ is 1 if $s = t$ and 0 otherwise. We say that $\hat{a}(\omega)$ is *bigger* than $\hat{a}(\omega')$ if $|\hat{a}(\omega)| > |\hat{a}(\omega')|$. The *energy* of $\mathbf{a}$ is $\|\mathbf{a}\|_2^2$. We also refer to $|\hat{a}(\omega)|^2$ as the energy of the Fourier coefficient $\hat{a}(\omega)$ (or the energy of ω) and, similarly, the energy of a set of Fourier coefficients is the sum of the squares of their magnitudes.

We write $\mathbf{f} \star \mathbf{g}$ to denote the convolution, $(\mathbf{f} \star \mathbf{g})(t) = \sum_s f(s) g(t-s)$. It follows that $\widehat{\mathbf{f} \star \mathbf{g}} = \hat{\mathbf{f}}\hat{\mathbf{g}}$. Parsefal's equality says that $\sum_t |f(t)|^2 = \sum_\omega |\hat{f}(\omega)|^2$. We have $\cos(x) = (e^{ix} + e^{-ix})/2$. We denote by χ_S the signal that equals 1 on S and zero elsewhere. The index to χ_S may be time or frequency; this is made clear from context. For more background on Fourier analysis, see [11].

For small real $\epsilon > 0$, we will write $\tilde{x} = (1 \pm \epsilon)x$ to mean $|\tilde{x} - x| \leq \epsilon |x|$, where $|x|$ is the complex absolute value. It is not necessary that the complex-valued $\tilde{x}$ be a real multiple of the complex-valued x.

We have the following access to $\mathbf{a}$. We toss coins, then, based on the coins, compute a set $T \subseteq [0, N)$ of indices, and learn $a(t)$ for $t \in T$. Thus, for example, we could pick t at random and then learn $a(t), a(t+1)$, and $a(t+2)$, so that the samples are dependent. We cannot adapt our choice of sample to the values seen. Our goal is to bound the time used by the algorithm, which implies a bound on the number of samples made.

If $\mathbf{a}$ contains large or precise entries, we will need extra time and space (polynomial in the input size) just to read and process input samples. Similarly, if $\mathbf{a}$ is exactly or very nearly representable by B coefficients, we will need time and space to perform computations precise enough to capture $\mathbf{a}$ as well as we claim or as well as desired (in the case of an exact superposition). Let M be a crude upper bound on $\|\mathbf{a}\|_2$ divided by the precision unit (note that $\|\mathbf{a}\|_2 \geq \|\mathbf{a}\|_\infty$, the maximum size of input values.) We assume that we know M. Our time bounds will all contain an unavoidable factor of $\log(M)$, and, when we need to reuse a set of samples $\log(M)$ times, we need to increase the size of the sample set by the factor $\log\log(M)$ to keep the probability of failure low.

Let $c(N) \leq 2^{N^{o(1)}}$ be any increasing function. Then any sampling algorithm that, on input a vector $\mathbf{f}$ of length N, distinguishes $\|\mathbf{f}\|_2^2 \leq 1$ from $\|\mathbf{f}\|_2^2 \geq c(N)$, makes $\log(M) N^{1-o(1)}$ samples. This is because suppose $\mathbf{f} = c(N)\delta_t$, for some randomly chosen t. It is easy to see that an algorithm that distinguishes $\mathbf{f}$ from 0 makes $\Omega(N) \geq \log(M) N^{1-o(1)}$ samples.

Our algorithms are randomized. That is, for all inputs $\mathbf{a}$ and $3/4$ of the random choices of our algorithm, the algorithm succeeds. The success probability $3/4$ ("significant") can be boosted to as close to 1 as desired ("high") using standard inexpensive techniques, that we rarely discuss further.

3 An Ideal Algorithm

In this section we present an idealized greedy pursuit (IGP) algorithm for finding a near-optimal Fourier representation. While IGP is not feasible in the sampling model, it can be modified appropriately. These modifications form the bulk of our technical contribution and will be discussed in the next section. The main components of IGP are, however, crucial for the feasible algorithm and it is illustrative to specify them precisely. The three main components of IGP are:

- *Identification* of all frequencies ω that contribute significantly to the signal's energy ($|\hat{a}(\omega)|^2$ is large);
- *Estimation* of $\hat{a}(\omega)$ when $|\hat{a}(\omega)|$ is large (call this estimate $\tilde{\hat{a}}(\omega)$);
- *Iteration* on the residual signal $\mathbf{a} - \tilde{\hat{a}}(\omega)\psi_\omega$ (*i.e.*, we add the representation for $\mathbf{a} - \tilde{\hat{a}}(\omega)\psi_\omega$ to $\tilde{\hat{a}}(\omega)\psi_\omega$).

3.1 Ideal Greedy Pursuit

In the ideal setting, the *estimation* step is exact and the *iteration* step is simply greedy pursuit. That is, we assume that, once we have identified a significant frequency ω_0, we have some technique to compute $\hat{a}(\omega_0)$ exactly. Because the Fourier basis $\{\psi_\omega\}$ is an orthonormal one, the best B-term representation for $\mathbf{a}$ is the best 1-term representation $\hat{a}(\omega_0)\psi_{\omega_0}$, plus the best $(B-1)$-term representation for $\mathbf{a} - \hat{a}(\omega_0)\psi_{\omega_0}$ (in which ω_0 is absent). We greedily add $\hat{a}(\omega_0)\psi_{\omega_0}$ to a growing representation $\mathbf{r}$ and iterate on $\mathbf{a} - \hat{a}(\omega_0)\psi_{\omega_0}$.

While the *estimation* and *iteration* steps have direct analogs in the sampling model, the *identification* step, however, does not. We now consider more closely two components of *identification*, namely *group testing* and *isolation*, that have direct analogs.

Group Testing. We assume initially that $\mathbf{a}$ consists of one pure frequency ω_0 plus orthogonal terms of insignificant energy; $\mathbf{a} = \hat{a}(\omega_0)\psi_{\omega_0} + \rho$ with $\langle \psi_{\omega_0}, \rho \rangle = 0$ and $\|\rho\|_2^2 \leq (0.25)\|\mathbf{a}\|_2^2$. Our goal is to identify ω_0. We will make progress towards this goal by repeatedly halving a list of candidates that always contains ω_0.

Consider the vector $\hat{\mathbf{a}}\chi_{\left[0,\frac{N}{2}\right)}$ consisting of the first $N/2$ Fourier coefficients of $\mathbf{a}$. Observe that, if $\omega_0 \in [0, N/2)$, then $\left\|\hat{\mathbf{a}}\chi_{\left[0,\frac{N}{2}\right)}\right\|_2^2 \geq |\hat{a}(\omega_0)|^2 \geq (0.75)\|\hat{\mathbf{a}}\|_2^2$, and

$$\left\|\hat{\mathbf{a}}\chi_{\left[\frac{N}{2},N\right)}\right\|_2^2 \leq \|\rho\|_2^2 \leq (0.25)\|\hat{\mathbf{a}}\|_2^2 < \left\|\hat{\mathbf{a}}\chi_{\left[0,\frac{N}{2}\right)}\right\|_2^2. \tag{1}$$

Thus, by *grouping* the first and second halves of the spectrum of $\mathbf{a}$ with two filters $\chi_0 = \chi_{\left[0,\frac{N}{2}\right)}$ and $\chi_1 = \chi_{\left[\frac{N}{2},N\right)}$ and by *testing* whether the energy of the first half is greater than or less than the energy of the second half, we cut in half the number of possibilities for ω_0. Note that we can compute $\|\hat{\mathbf{a}}\chi_0\|_2^2$ in the time domain as $\|\mathbf{a} \star \check{\chi}_0\|_2^2$, where $\check{\chi}_0$ is the inverse Fourier transform of χ_0. (Even in this infeasible algorithm, we don't want to compute $\hat{\mathbf{a}}$ directly.)

Suppose, without loss of generality, that $\omega_0 \in [0, N/2)$; *i.e.*, the most significant bit of ω_0 is 0. We now adaptively seek the second most significant bit. To do this, define $\mathbf{f}(t) = \mathbf{a}(t/2)$. It follows

that the sequence $\hat{a}(0), \hat{a}(1), \hat{a}(2), \ldots, \hat{a}(N/2-1)$ is mapped to $\hat{f}(0), \hat{f}(2), \hat{f}(4), \ldots, \hat{f}(\approx N)$, and the other (low-energy) frequencies of $\hat{\mathbf{a}}$ in $[N/2, N)$ are mapped to positions $1, 3, 5, \ldots$. We repeat the most significant bit test for the big frequencies of $\mathbf{f}$, learning the *second* most significant bit of ω_0. Continuing this way, we learn all of ω_0.

Isolation. The group-testing procedure is successful if $\mathbf{a}$ consists predominantly of one pure tone. On the other hand, if, for example, $\mathbf{a}$ comprises two pure frequencies, each with $1/3$ the total energy, plus orthogonal noise at $1/3$ the energy, group testing will fail to find directly either frequency. From a test that tells us that some significant frequency is in $S_1 \subseteq [0, N)$ and another test that tells us that $S_2 \subseteq [0, N)$ contains a significant frequency, we cannot conclude that $S_1 \cap S_2$ contains a big frequency. This is in contrast to the situation of a single overwhelmingly energetic tone. We proceed by isolating big Fourier coefficients first then using group testing to identify them precisely.

Assume that $\mathbf{a}$ consists of one or more pure tones plus orthogonal noise but that the energy of the pure tones is no longer overwhelming. That is, $\mathbf{a} = \psi + \rho$ with $\langle \psi, \rho \rangle = 0$ and $\|\psi\|_2^2 \geq \eta \|\mathbf{a}\|_2^2$, but η is considerably less than 1/2. We seek a frequency ω_0 such that $|\hat{a}(\omega_0)|^2 \geq \eta \|\mathbf{a}\|_2^2$.

From $\mathbf{a}$, first construct a vector $R\mathbf{a}$ such that the spectrum of $R\mathbf{a}$ is a random permutation of the spectrum of $\mathbf{a}$. Now, consider the family of functions $\mathbf{f}_j$, $j = 0, \ldots, 1/\eta^2$, obtained by filtering $R\mathbf{a}$ with the filters $\chi_j = \chi_{[j\eta^2 N, (j+1)\eta^2 N)}$ in the frequency domain. Note that each $\hat{\mathbf{f}}_j$ consists of (at most) $\eta^2 N$ non-zero coefficients that form a random subset of $\eta^2 N$ coefficients of $\hat{\mathbf{a}}$. One can show that, with significant probability, each of the frequencies ω_i of $\mathbf{a}$ that contains energy at least $\eta \|\mathbf{a}\|_2^2$ is *isolated* to one $\mathbf{f}_{j_i}$, and all frequencies are isolated this way. Furthermore, we show that each coefficient satisfies $|\hat{\mathbf{f}}_{j_i}(\omega_i)|^2 \geq (0.75)\|\mathbf{f}_{j_i}\|_2^2$, so we can appeal to the previous group testing procedure to identify ω_i precisely.

3.2 Infeasible Aspects of IGP

There are several aspects of IGP that are infeasible in the sampling model. In particular, as we know, a sampling algorithm cannot estimate $\|\mathbf{a}\|_2^2$ or other norms well. For many aspects of IGP, estimation of norms is part of a straightforward implementation; fortunately, it is not necessary for all implementations. In addition, although a sampling algorithm can produce a representation $\mathbf{r}$ that is near optimal, the algorithm has no way to assess the error $\|\mathbf{a} - \mathbf{r}\|_2^2$.

The infeasible aspects are:

- We cannot compute $\hat{a}(\omega)$ exactly, nor even with good relative error. This also affects *identification* (we can't always resolve which coefficient is largest) and *iteration* (frequency ω may appear in $\mathbf{a} - \tilde{\hat{a}}(\omega)\psi_\omega$; ω may even dominate).

- We cannot directly compare $\left\| \hat{\mathbf{a}} \chi_{[0, \frac{N}{2})} \right\|_2^2$ with $\left\| \hat{\mathbf{a}} \chi_{[\frac{N}{2}, N)} \right\|_2^2$ since a sampling algorithm cannot, in general, estimate norms, even to within huge relative or additive error, as we show below.

- The vector $\mathbf{a} \star \check{\chi}$ is too expensive to compute by sampling, even approximately, since each point of $\mathbf{a} \star \check{\chi}$ depends significantly on most points of $\mathbf{a}$. (Our goal is to sample just a few points of $\mathbf{a}$.)

- Constructing $R\mathbf{a}$ to have spectrum that is a truly random permutation of $\mathbf{a}$'s spectrum is too expensive for a sampling algorithm.

4 A Feasible Algorithm

In the previous section, we listed four aspects of IGP that are infeasible in the sampling model. In this section we address those problems with specific technical modifications. In Section 4.1, we show how to estimate $\hat{a}(\omega)$ as $\tilde{\hat{a}}(\omega)$, with $|\hat{a}(\omega) - \tilde{\hat{a}}(\omega)|^2 \leq \epsilon \|\mathbf{a}\|_2^2$. In Section 4.2, we show that a sampling algorithm can get upper and lower bounds on L^2 norms, that happen to be good enough to perform the analog of the comparison of norms in (1). In Sections 4.3 and 4.4, we show how to perform *identification* and *isolation* using time-limited filters suitable for a sampling algorithm (as opposed to $\chi^\vee$). There we use a pairwise-independent permutation of the spectrum of $\mathbf{a}$. Finally, in Section 4.5, we analyze the resulting greedy pursuit algorithm. In this extended abstract, all proofs appear in an appendix.

4.1 Estimating Individual Fourier Coefficients

Lemma 2 *There exists a sampling algorithm A with cost $O(\log(M)/\epsilon)$ such that, for each frequency ω and each vector $\mathbf{a}$ of length N, and each $\epsilon > 0$, with high probability, the output of A on input $(\mathbf{a}, \omega, \epsilon)$ is $\tilde{\hat{a}}(\omega)$ with $|\tilde{\hat{a}}(\omega) - \hat{a}(\omega)|^2 \leq \epsilon \|\mathbf{a}\|_2^2$.*

Pick $O(1/\epsilon)$ copies of t uniformly at random and let $\mathbf{a}' = N\mathrm{avg}(a(t)\delta_t)$. Put $\tilde{\hat{a}}(\omega) = \hat{a'}(\omega)$. A full proof of correctness appears in the appendix. We note that the sample points need only to be pairwise independent. For example, the sample points could be the elements of an arithmetic progression of length $O(1/\epsilon)$ with random starting point and random common difference.

4.2 Estimating Norms

We turn now to estimating norms by sampling.

Lemma 3 *There's a sampling algorithm, A, that takes a bound M on $\|\mathbf{f}\|_2$, makes $O(\log\log(M))$ samples and runs in time polynomial in $\log(M)$, such that, on input $\mathbf{f}$ with length N with biggest Fourier coefficient $\hat{f}(\omega)$, A produces, with high probability, a random output X such that*

1. *$X \leq \|\mathbf{f}\|_2^2$ (for any $\mathbf{f}$).*
2. *If $|\hat{f}(\omega)|^2 \geq 0.95\|\mathbf{f}\|_2^2$, then $X \geq 0.5\|\mathbf{f}\|_2^2$.*

Intuitively, the proof is as follows. For random $t \in [0, N)$, let $Y = N|f(t)|^2$ be a random variable. Then $E[Y] = \|\mathbf{f}\|_2^2$; we need to analyze the variance. If $\mathbf{f}$ has a small number of spikes, we are likely to miss the spikes, thus underestimating $\|\mathbf{f}\|_2^2$, but, otherwise, the variance is small and Y will be a good estimate. In fact, we *must* miss the spikes—if our algorithm gets a big sample value, that may be a spike, the algorithm pretends that this value is zero. By the uncertainty principle, this does not greatly affect the final representation. This gives the first statement. If $\mathbf{f}$ is a pure frequency (which has no spikes—in fact, $|\psi|$ is constant for pure frequencies), then Y is always

exactly equal to $\|\mathbf{f}\|_2^2$. Even if only 95% of $\mathbf{f}$ is a pure frequency, sufficient energy of $\mathbf{f}$ is away from spikes that the sampling estimate is good. (The numerical value $0.5\|\mathbf{f}\|_2^2$ comes about because it is less than $(\sqrt{0.95} - \sqrt{1-0.95})^2\|\mathbf{f}\|_2^2$.) Thus the success of the second statement is a direct consequence of the uncertainty principle.

4.3 Group Testing

Recall that, in the ideal algorithm, for *identification*, we used filter functions defined in the frequency domain by $\chi_{\left[0,\frac{N}{2}\right)}$ and $\chi_{\left[\frac{N}{2},N\right)}$. In this section, we first define imperfect filter functions based on cosines that will be easier for a sampling algorithm to use, then show how to use them.

Lemma 4 *For $0 \leq k < 16$, let $\hat{g}_k(\omega) = (1 + \cos(2\pi\omega/N - 2\pi k/16))/2$. Then the inverse Fourier transform of $\hat{\mathbf{g}}_k$ is given by $g_k(t) = \frac{\sqrt{N}}{2} e^{2\pi i k t/16}$ for $t = \pm 1$, $g_k(0) = \sqrt{N}$, and $g_k(t) = 0$ otherwise.*

Proof: Immediate. ∎

Thus, for all k, $(\mathbf{f} \star \mathbf{g}_k)(t)$ is a linear combination of three values of $\mathbf{f}$, and can be sampled efficiently by an algorithm that samples $\mathbf{f}$.

Definition 5 Denote by pass_k the set $\{\omega : |2\pi\omega/N - 2\pi k/16| \leq 2\pi/32\}$. ∎

Thus pass_k consists of the ω's within $1/32$ of a period to the maximum of $\hat{\mathbf{g}}_k$. Note that, for $\omega \in \mathrm{pass}_k$, $\hat{g}_k(\omega) \geq (\cos(2\pi/32) + 1)/2 \geq 0.99$. (See Figure 2 in the appendix.)

We turn now to group testing. In this section, we assume $\mathbf{f}$ consists mainly of a single frequency:

Definition 6 Let $\mathcal{F}$ denote the class of complex-valued vectors $\mathbf{f}$ of length N, such that, for some ω and some complex number b, $\mathbf{f} = \psi + \rho$, where $\langle \psi, \rho \rangle = 0$, $\psi = b\psi_\omega$ is a pure frequency, and $\|\psi\|_2^2 \geq (0.98)\|\mathbf{f}\|_2^2$. For $\mathbf{f} \in \mathcal{F}$, we say that $\mathbf{f}$ is "98% pure." ∎

Finally, we also need the following transform on $\mathbf{f}$, that scales and translates $\hat{\mathbf{f}}$.

Definition 7 Define $R_{\theta,\sigma}\mathbf{f}$ by $R_{\theta,\sigma} f(t) = e^{-2\pi i \theta t/N} f(t/\sigma)$. Thus $\widehat{(R_{\theta,\sigma} f)}(\omega) = \hat{f}(\sigma\omega + \theta)$. ∎

Lemma 8 *There is a sampling algorithm, A, with time and sample complexity $\log(M)\log^{O(1)}(N)$, such that, on input a 98% pure vector $\mathbf{f}$ of length N, A identifies the frequency ω' of the biggest Fourier coefficient of $\mathbf{f}$.*

We proceed as in the group testing procedure of IGP, except we use cosines $\hat{\mathbf{g}}_k$ instead of characteristic functions. To learn the most significant bit of ω' we use $\hat{\mathbf{g}}_k$ instead of $\chi_{\left[0,\frac{N}{2}\right)}$. We will use "band-pass" regions pass_k of $\mathbf{g}_k$ with size $N/16$ and antipodal "band-reject" regions with size $9N/16$, so we have to use all 16 filters $\hat{\mathbf{g}}$ together to complete this test. To learn the second most significant bit of ω' after learning the most significant (and assuming, without loss of generality, $-N/4 < \omega' < +N/4$), we dilate $\mathbf{f}$ by 2 and apply the 16 filters again. Continuing this way, we learn ω'.

We note that, although our algorithm adapts to signal values (*e.g.*, by immediately multiplying an observed sample $a(t)$ by a phase shift $e^{2\pi i\theta t/N}$, where θ depends on previously-observed signal values), the set of samples made by our algorithm is non-adaptive.

4.4 Isolation

Finally, we consider *isolation* of the significant coefficients, the last part of *identification*. That is, we are given a signal $\mathbf{a} = \psi + \rho$, where ψ is a pure frequency $\psi = b\psi_{\omega'}$, $\langle \psi, \rho \rangle = 0$, and $\|\psi\|_2^2 \geq \eta \|\mathbf{a}\|_2^2$, where $\eta > 0$ may be much less than 0.98—even much less than $1/2$. Our goal is to output a short list of frequencies that contains ω'. To that end, we construct a short sequence $\mathbf{f}_0, \mathbf{f}_1, \ldots$ of signals, such that, for some j, $|\hat{f}_j(\omega')|^2 \geq 0.98\|\mathbf{f}_j\|_2^2$. We can then use the techniques of previous sections on each $\mathbf{f}_j$ to identify a candidate for ω'. The following filter function will be used for isolation. (See Figure 3, in the appendix.)

Definition 9 [Fejér] For integer k, define $\mathbf{h}_k$ by $h_k(t) = \frac{\sqrt{N}}{2k+1}\chi_{[-k,k]}$. ∎

Lemma 10 *We have the following.*

1. *For all k,*

$$\hat{h}_k(\omega) = \frac{1}{2k+1}\sum_{t=-k}^{k} e^{-2\pi i \omega t/N} = \begin{cases} \frac{\sin(\pi(2k+1)\omega/N)}{(2k+1)\sin(\pi\omega/N)}, & \omega \neq 0 \\ 1, & \omega = 0. \end{cases}$$

2. *For all k and all ω, $|\hat{h}_k(\omega)| \leq 1$.*

3. *For all k and ω such that $|\omega| \leq \frac{N}{2(2k+1)}$, we have $\hat{h}_k(\omega) \geq 2/\pi$.*

4. *For all k, $\|\hat{\mathbf{h}}_k\|_2^2 = \frac{N}{2k+1}$.*

Proof: All immediate. ∎

We now show how to use $\mathbf{h}_k$, for appropriate k, to isolate frequencies. In this section, we again assume that N is prime. The techniques of this section can be modified to work for all N.

Lemma 11 *Suppose θ and σ are chosen randomly mod N, with σ invertible. Then $\omega \mapsto \sigma\omega + \theta$ is a pairwise-independent permutation of $\hat{a}$. That is, if $\omega_1 \neq \omega_2$ and $\omega_3 \neq \omega_4$, then $\omega_1 \mapsto \omega_3$ and $\omega_2 \mapsto \omega_4$ with probability $\frac{1}{N} \cdot \frac{1}{N-1}$.*

Proof: Immediate. ∎

Note that $\widehat{R_{\theta,\sigma}a}(\omega) = \hat{a}(\sigma\omega + \theta)$.

Lemma 12 *Given signal $\mathbf{a}$ and number η we can create $2k+1$ new signals, $\mathbf{f}_0, \ldots, \mathbf{f}_{2k}$, such that:*

- *For each ω' such that $|\hat{a}(\omega')|^2 \geq \eta\|\mathbf{a}\|_2^2$, there exists a j such that $|\hat{f}_j(\omega')|^2 \geq 0.98\|\mathbf{f}_j\|_2^2$.*
- *Each $\mathbf{f}_j$ can be sampled by sampling non-adaptively from $\mathbf{a}$ in $O(k)$ places.*
- *k is small,* i.e.*, $k \leq O(1/\eta)$.*

Pick θ and σ at random, with σ invertible. Let $k \leq O(1/\eta)$ be sufficiently large. Then consider the signal $\mathbf{f}_j = (e^{2\pi i j t/(2k+1)}\mathbf{h}_k) \star R_{\theta,\sigma}\mathbf{a}$, for $0 \leq j < 2k+1$. Semantically, $\hat{\mathbf{f}}_j$ is formed by starting with $\hat{\mathbf{a}}$, performing a pairwise-independent permutation (in the frequency domain), then multiplying pointwise by a phase shift of $\hat{\mathbf{h}}_k$ by $jN/(2k+1)$. The "pass" regions of $e^{2\pi i j t/(2k+1)}\mathbf{h}_k$ partition $[0, N)$. If ω' is in the "pass" region of the j'th filter, then $|\hat{f}_j(\sigma\omega' + \theta)|^2 \geq (\eta/4)\|\mathbf{a}\|_2^2$. We show that, with significant probability, $\|\mathbf{f}\|_2^2 - |\hat{f}_j(\sigma\omega' + \theta)|^2 \leq (\eta/200)\|\mathbf{a}\|_2^2$.

4.5 Adaptive Greedy Pursuit

Above we showed, for any ϵ and B, given an $\mathbf{a}$, we can construct a short list of frequencies that contains all ω' such that $|\hat{a}(\omega')|^2 \geq \eta\|\mathbf{a}\|_2^2$, for appropriate η. Using Lemma 2, we can estimate the value of each corresponding coefficient to within $\eta\|\mathbf{a}\|_2$, additively. In this section, we show that this suffices for an adaptive greedy algorithm.

Theorem 13 *Fix a signal* $\mathbf{a}$*. Suppose, for all representations* $\mathbf{r}'$ *of at most* B *terms, we can, with cost* $1/\eta^{O(1)}$*,*

- *estimate* $\widehat{\mathbf{a}-\mathbf{r}'}(\omega)$ *as* $\widehat{\tilde{\mathbf{a}-\mathbf{r}'}}(\omega)$ *with* $|\widehat{\mathbf{a}-\mathbf{r}'}(\omega) - \widehat{\tilde{\mathbf{a}-\mathbf{r}'}}(\omega)|^2 \leq \eta\|\mathbf{a}\|_2^2$
- *output a list of at most* $1/\eta^{O(1)}$ *frequencies that contains all frequencies* ω *such that* $|\widehat{\mathbf{a}-\mathbf{r}'}(\omega)|^2 \geq \eta\|\mathbf{a}-\mathbf{r}'\|_2^2$.

Then we can, on input B *and* ϵ*, with cost* $(B\log(N)\log(M)/\epsilon)^{O(1)}$*, output a* B*-term representation* $\mathbf{r}$ *with sum-square-error* $\|\mathbf{a}-\mathbf{r}\|_2^2 \leq (1+\epsilon)\|\mathbf{a}-\mathbf{r}_{\text{opt}}\|_2^2$*, where* $\mathbf{r}_{\text{opt}}$ *is the* B*-term representation for* $\mathbf{a}$ *with the least sum-square-error.*

We use the greedy algorithm of Figure 4. This is the classic greedy pursuit algorithm, except:

- When searching for a new coefficient for our representation, we cannot find the biggest coefficient, only a near-biggest. Since (in this variant of greedy pursuit) we have no facility to eject a wrongly-chosen coefficient, we need to argue that each coefficient we take is acceptable.
- Our algorithm revisits frequencies, so it cannot halt after B steps. Furthermore, unlike a classic algorithm that can measure its progress and can halt when no further improvement is possible, our algorithm in general continues even after no further progress is possible. We need to show that potential extraneous rounds of greedy pursuit performed by our algorithm don't worsen things by much.

Each of these is straightforward to check. For completeness, we present the entire greedy pursuit algorithm in the appendix.

5 Assessing our Representation's Quality

Unfortunately, a sampling-only algorithm has no way to assess the error $\|\mathbf{a}-\mathbf{r}\|_2^2$ of the output representation $\mathbf{r}$. For example, if $\mathbf{a} = b\delta_s$ is a spike in time at s, a sampling algorithm will miss s altogether, and can not estimate b, the error of the output representation $\mathbf{r} = 0$ (which is near-best in this case). We now show that, if we happen to know a good approximation to $\|\mathbf{a}\|_2^2$, then we *can* assess the quality, at least roughly.

Lemma 14 *Suppose* $\mathbf{r}$ *is a representation for* $\mathbf{a}$ *such that* $\|\mathbf{a}-\mathbf{r}\|_2^2 \leq (1+\epsilon)\|\mathbf{a}-\mathbf{r}_{\text{opt}}\|_2^2$*. Then* $\|\mathbf{a}-\mathbf{r}\|_2^2 = \|\mathbf{a}\|_2^2 - \|\mathbf{r}\|_2^2 \pm 4\sqrt{\epsilon}\|\mathbf{a}\|_2^2$.

6 Conclusion

We provide a sampling algorithm that yields a B-term Fourier representation $\mathbf{r}$ for any input signal $\mathbf{a}$ of length N, with the guarantee that $\|\mathbf{a}-\mathbf{r}\|_2^2$ is within a factor $(1+\epsilon)$ of the best possible B-term Fourier representation. The number of samples is at most $\mathrm{poly}(B\log(N)\log(M)/\epsilon)$ and these sample positions are independent of the signal. The three main components of this algorithm are the *identification* of significant frequencies, the *estimation* of the Fourier coefficients corresponding to the significant frequencies, and finally *iteration* on the residual representation.

This algorithm has important applications in two major areas: mathematics and theoretical computer science. First, this algorithm hints at the looseness of the Uncertainty Principle when the time and frequency index sets are chosen at random. It also suggests that many standard algorithms in computational Fourier analysis (especially signal recovery) may be dramatically improved through the use of randomness. Second, we can use this algorithm as an oracle to produce a near-optimal Fourier representation for a signal projected onto a given interval. This allows a dynamic programming algorithm to produce a piecewise Fourier representation with near-optimal boundaries and coefficients. Such an algorithm can be used in data mining (*e.g.*, to find approximate periodic behavior) and in speech analysis (*e.g.*, to track *formants*).

Acknowledgments

For helpful discussions, we thank: Ingrid Daubechies, Ron DeVore, Sinan Güntürk, and Henry Landau.

References

[1] D. Achlioptas, F. McSherry: Fast computation of low rank matrix. STOC 2001: 611-618.

[2] N. Alon, Y. Matias, and M. Szegedy, The Space Complexity of Approximating the Frequency Moments. In *Proceedings of the 28th Annual ACM Symposium on Theory of Computing* (STOC), pp. 20–29, May 1996.

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

[4] A. Frieze, R. Kannan and S. Vempala. Fast Monte-Carlo Algorithms for Finding Low-Rank Approximations. Proc. of the 39th Foundations of Computer Science (FOCS '98), Palo Alto, 1998.

[5] A. C. Gilbert, S. Guha, P. Indyk, Y. Kotidis, S. Muthukrishnan, and M. J. Strauss. Fast, Small-Space Algorithms for Approximate Histogram Maintenance. 2001, Manuscript.

[6] W. B. Johnson and J. Lindenstrauss. 'Extensions of Lipshitz mapping into Hilbert space. *Contemporary Mathematics*, **26** 189–206, 1984.

[7] E. Kushilevitz, Y. Mansour: Learning Decision Trees Using the Fourier Sprectrum. STOC 1991: 455-464.

[8] N. Linial, Y. Mansour, N. Nisan. Constant Depth Circuits, Fourier Transform, and Learnability. JACM 40(3): 607-620 (1993).

[9] Y. Mansour. Learning Boolean Functions via the Fourier Transform. In *Theoretical Advances in Neural Computation and Learning*, (V.P. Roychodhury and K-Y. Siu and A. Orlitsky, ed.), 391–424 (1994).

[10] C. E. Shannon. Communications in the presence of noise. In *Proc. of the IRE*, vol. 37, pp. 10–21, January 1949.

[11] H. J. Weaver. *Applications of Discrete and Continuous Fourier Analysis*. Wiley, 1983.

Appendix

A Variants

We first consider an algorithm based solely on Lemma 2. Make $O(B\log(N)/\epsilon)$ samples from $\mathbf{a}$. For each frequency ω, estimate $\hat{a}(\omega) \pm \sqrt{\epsilon/B}\|\mathbf{a}\|_2$ using Lemma 2. Output the representation consisting of the B largest coefficients.

First, the usefulness: This algorithm makes just a small number of samples from $\mathbf{a}$. Furthermore, one can show that the output representation, $\mathbf{r}$, satisfies $\|\mathbf{a}-\mathbf{r}\|_2^2 \leq \|\mathbf{a}-\mathbf{r}_{\rm opt}\|_2^2 + \epsilon\|\mathbf{a}\|_2^2$. The main advantage of this algorithm is its simplicity—it avoids sampling-based identification and greedy pursuit. Unfortunately, there are two drawbacks. First, the algorithm takes $\Omega(N)$ time, which is prohibitive in some applications. Also, the error bound, $\epsilon\|\mathbf{a}\|_2^2$ may be much worse than $\epsilon\|\mathbf{a}-\mathbf{r}_{\rm opt}\|_2^2$ (and, in fact, the actual error may much worse than $\epsilon\|\mathbf{a}-\mathbf{r}_{\rm opt}\|_2^2$). Still, if $\mathbf{r}_{\rm opt}$ is only moderately good (so that $\epsilon\|\mathbf{a}-\mathbf{r}_{\rm opt}\|_2^2$ and $\epsilon\|\mathbf{a}\|_2^2$ are comparable), and sample cost but not time cost is an issue, then this simple algorithm suffices.

Next, consider using Lemma 2 to estimate coefficients, then using the greedy algorithm of Section 4.5 to produce a representation. As discussed above, this gives a near optimal representation. Also, the number of samples to $\mathbf{a}$ is small. This variant requires time $\Omega(N)$, but avoids sampling-based identification, which increases the sample complexity. This variant is appropriate for information-theoretic analysis and comparisons with classic uncertainty principles.

B Proofs

Lemma 2 *There exists a sampling algorithm A with cost $O(\log(M)/\epsilon)$ such that, for each frequency ω and each vector a of length N, and each $\epsilon > 0$, with significant probability, the output of A on input $(\mathbf{a}, \omega, \epsilon)$ is $\tilde{\hat{a}}(\omega)$ with $|\tilde{\hat{a}}(\omega) - \hat{a}(\omega)|^2 \leq \epsilon\|\mathbf{a}\|_2^2$.*

Proof: Pick t uniformly at random and let $\mathbf{a}' = Na(t)\delta_t$. Then we have

$$\begin{aligned} E[\hat{a'}(\omega)] &= \frac{1}{N}\sum_t \langle Na(t)\delta_t, \psi_\omega\rangle \\ &= \sum_t a(t)\,\langle\delta_t, \psi_\omega\rangle \\ &= \hat{a}(\omega). \end{aligned}$$

Also,

$$\begin{aligned} E[|\hat{a'}(\omega)|^2] &= \frac{1}{N}\sum_t |\langle Na(t)\delta_t, \psi_\omega\rangle|^2 \\ &= N\sum_t |a(t)|^2 |\langle \delta_t, \psi_\omega\rangle|^2 \\ &= N\sum_t |a(t)\overline{\psi_\omega(t)}|^2 \\ &\leq \sum_t |a(t)|^2, \quad \text{since } |\psi_\omega|^2 \leq O(1/N). \end{aligned}$$

Thus, if we take an average of $O(1/\epsilon)$ independent copies of a' and compute the average of $\hat{a'}(\omega)$, the result, X, has $E[X] = \hat{a}(\omega)$ and $E[|X|^2] \leq O(\epsilon\|\mathbf{a}\|_2^2)$. The result follows by the Chebychev inequality. ∎

We note that the sample points need only to be pairwise independent. For example, the sample points could be the elements of an arithmetic progression of length $O(1/\epsilon)$ with random starting point and random common difference.

Lemma 3 *There's a sampling algorithm, A, that takes a bound M on $\|\mathbf{f}\|_2$, makes $O(\log\log(M))$ samples and runs in time polynomial in $\log(M)$, such that, on input $\mathbf{f}$ of length N with biggest Fourier coefficient $\hat{f}(\omega)$, A produces, with high probablility, a random output X such that*

1. *$X \leq \|\mathbf{f}\|_2^2$ (for any $\mathbf{f}$).*
2. *If $|\hat{f}(\omega)|^2 \geq 0.95\|\mathbf{f}\|_2^2$, then $X \geq 0.5\|\mathbf{f}\|_2^2$.*

Intuitively, the proof is as follows. For random $t \in [0, N)$, let $Y = N|f(t)|^2$ be a random variable. Then $E[Y] = \|\mathbf{f}\|_2^2$; we need to analyze the variance. If $\mathbf{f}$ has a small number of spikes, we are likely to miss the spikes, thus underestimating $\|\mathbf{f}\|_2^2$, but, otherwise, the variance is small and Y will be a good estimate. In fact, we *must* miss the spikes—if our algorithm gets a big sample value, that may be a spike, the algorithm pretends that this value is zero. By the uncertainty principle, this does not greatly affect the final representation. This gives the first statement. If $\mathbf{f}$ is a pure frequency (which has no spikes—in fact, $|\psi|$ is constant for pure frequencies), then Y is always exactly equal to $\|\mathbf{f}\|_2^2$. Even if only 95% of $\mathbf{f}$ is a pure frequency, sufficient energy of $\mathbf{f}$ is away from spikes that the sampling estimate is good. (The numerical value $0.5\|\mathbf{f}\|_2^2$ comes about because it is less than $(\sqrt{0.95} - \sqrt{1-0.95})^2\|\mathbf{f}\|_2^2$.) Thus the success of the second statement is a direct consequence of the uncertainty principle.

Proof: For each number c, define $K_c\mathbf{f}$ ("$\mathbf{f}$ clipped at c") by

$$(K_c f)(t) = \begin{cases} f(t), & |f(t)| \leq c/\sqrt{N} \\ 0 & \text{otherwise.} \end{cases}$$

Let $\beta > 0$ be a small number (independent of N and M) that we will determine later. Perform the algorithm of Figure 1.

Figure 1: Approximation algorithm for $\|\mathbf{f}\|_2^2$. The parameters $\beta > 0$ and $k = k(\beta)$ are described in the text.

$c \leftarrow 2M/\beta$
Do
{
    $X \leftarrow \mathrm{avg}_k N|K_c f(t_k)|^2$ // each t_k chosen randomly and independently from $\{0, \ldots, N-1\}$
    $c \leftarrow \lfloor c/(1+\beta) \rfloor$
} while $X < \beta^2 c^2$
Output $X/(1+\beta)$.

First, the algorithm halts, since $c = 1$ is reached from an initial value of $c = 2M/\beta$, by constant-fraction reductions, and, on the next iteration, $c = 0$ and $K_0\mathbf{f} = 0$ so $X = 0 \not< 0 = \beta^2 c^2$.

It is easy to see that $E[X] = \|K_c\mathbf{f}\|_2^2$ as a loop invariant. Next,

$$\begin{aligned} E[|X|^2] &= \frac{1}{k}\frac{1}{N}\sum_{t=0}^{N} N^2 |K_c f(t)|^4 \\ &= \frac{N}{k}\sum_{t=0}^{N} |K_c f(t)|^4 \\ &\leq \frac{N}{k}\|K_c f\|_\infty^2 \sum_{t=0}^{N} |K_c f(t)|^2 \\ &\leq \frac{1}{k} c^2 \|K_c\mathbf{f}\|^2. \end{aligned}$$

Thus, with significant probability, $X = \|K_c\mathbf{f}\|_2^2 \pm O\left(\frac{1}{\sqrt{k}} c \|K_c\mathbf{f}\|_2\right)$.

As long as $\beta^2 c^2 \geq 2\|K_c\mathbf{f}\|_2^2$, and $k \leq O(1/\beta^2)$ is sufficiently large, $X < \beta^2 c^2$ with significant probability, so the algorithm will not halt. On the other hand, when $\beta^2 c^2 \leq 4\|K_c\mathbf{f}\|_2^2$, the variance of X is at most

$$\begin{aligned} \frac{1}{k} c^2 \|K_c\mathbf{f}\|_2^2 &\leq \frac{4}{\beta^2 k}\|K_c\mathbf{f}\|_2^4 \\ &\leq \beta^2 \|K_c\mathbf{f}\|_2^4, \end{aligned}$$

provided $k \geq 4/\beta^4$. It follows that

$$X = (1 \pm \beta)\|K_c\mathbf{f}\|_2^2 \tag{2}$$

is a good approximation to $\|K_c\mathbf{f}\|_2^2$. Thus, when the algorithm halts, $X/(1+\beta) \leq \|K_c\mathbf{f}\|_2^2 \leq \|\mathbf{f}\|_2^2$. This gives the first statement (and will also be used below).

Now, suppose $\mathbf{f} = \psi + \rho$, where $\psi = b\psi_\omega$ is a pure frequency, $\langle \psi, \rho \rangle = 0$ and $\|\rho\|_2^2 \leq 0.05\|\mathbf{f}\|_2^2$.

Consider c with $\|\psi\|_2^2 < \beta c^2$. Let $S = \{t : |f(t)| \geq c/\sqrt{N}\}$. Note that the sum of the $|f(t)|^2$ values is $\|\mathbf{f}\|_2^2$, so, by Markov's inequality, $|S| \cdot c^2/N \leq \|\mathbf{f}\|_2^2$, or

$$\begin{aligned} |S| &\leq N\|\mathbf{f}\|_2^2/c^2 \\ &\leq N(1.06)\|\psi\|_2^2/c^2 \\ &< N(1.06)\beta. \end{aligned}$$

(Note that $\|\psi\|_2^2 \geq (0.95)\|\mathbf{f}\|_2^2$ implies $\|\mathbf{f}\|_2^2 \leq (1.06)\|\psi\|_2^2$.) Thus, since $|\psi|$ is constant,

$$\begin{aligned} \left\|\psi\chi_{[0,N)\setminus S}\right\|_2^2 &= (1 - |S|/N)\|\psi\|_2^2 \\ &\geq (1 - 1.06\beta)\|\psi\|_2^2. \end{aligned}$$

Also, $\|\rho\chi_{[0,N)\setminus S}\|_2 \leq \|\rho\|_2$. It follows, using the triangle inequality, that

$$\begin{aligned} \|K_c\mathbf{f}\|_2 &= \left\|\mathbf{f}\chi_{[0,N)\setminus S}\right\|_2 \\ &\geq \left\|\psi\chi_{[0,N)\setminus S}\right\|_2 - \left\|\rho\chi_{[0,N)\setminus S}\right\|_2 \\ &\geq \sqrt{1 - 1.06\beta}\|\psi\|_2 - \|\rho\|_2 \\ &\geq \sqrt{1 - 1.06\beta}\sqrt{0.95}\|\mathbf{f}\|_2 - \sqrt{0.05}\|\mathbf{f}\|_2 \\ &\geq \sqrt{1 - 1.06\beta}(0.75)\|\mathbf{f}\|_2. \end{aligned}$$

Thus

$$\begin{aligned} \|K_c\mathbf{f}\|_2^2 &\geq (1 - 1.06\beta)(0.75)^2\|\mathbf{f}\|_2^2 \\ &\geq 0.52\|\mathbf{f}\|_2^2, \end{aligned} \tag{3}$$

for sufficiently small β.

Above we showed that, when the algorithm halts, X is a good approximation to $\|K_c\mathbf{f}\|_2^2$. That is, $X/(1+\beta) \geq \frac{1-\beta}{1+\beta}\|K_c\mathbf{f}\|_2^2$. Thus, if the algorithm halts for $\beta c^2 > \|\psi\|_2^2$,

$$\begin{aligned} X/(1+\beta) &\geq \frac{1-\beta}{1+\beta}\|K_c\mathbf{f}\|_2^2 \\ &\geq 0.52\frac{1-\beta}{1+\beta}\|\mathbf{f}\|_2^2 \\ &\geq 0.5\|\mathbf{f}\|_2^2, \end{aligned}$$

for sufficiently small β.

Finally, suppose $\|\psi\|_2^2 < \beta c^2 \leq 4\|\psi\|_2^2$. Since

$$\begin{aligned} \beta c^2 &\leq 4\|\psi\|_2^2 \\ &\leq 4\|\mathbf{f}\|_2^2 \\ &\leq 8\|K_c\mathbf{f}\|_2^2 \\ &\leq \frac{4}{\beta}\|K_c\mathbf{f}\|_2^2, \end{aligned}$$

it follows by (2) that $X = (1 \pm \beta)\|K_c\mathbf{f}\|_2^2$. By (3), $0.52\|\mathbf{f}\|_2^2 \leq \|K_c\mathbf{f}\|_2^2$, and, as above, it follows that $X \geq 0.5\|\mathbf{f}\|_2^2$. Thus

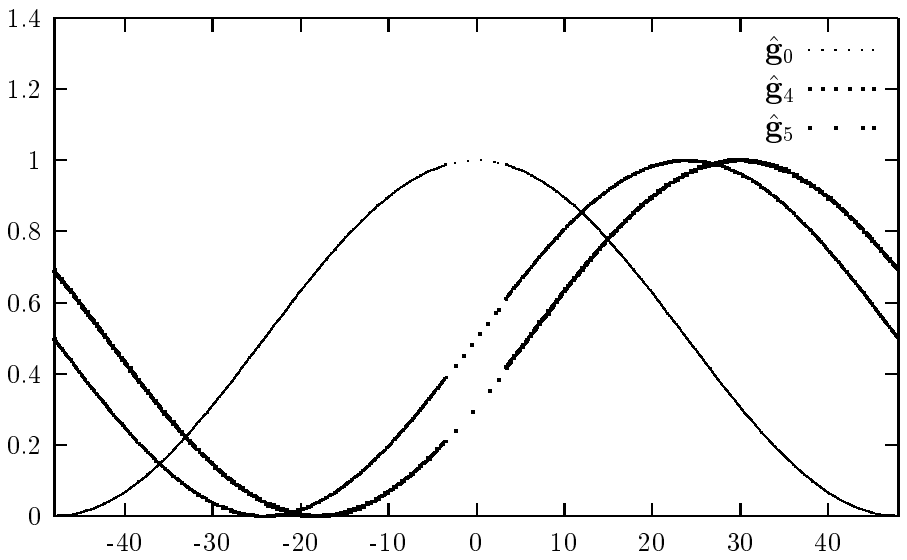
$$\begin{aligned} X &\geq 0.5\|\mathbf{f}\|_2^2 \\ &\geq 0.5\|\psi\|_2^2 \\ &\geq 0.5\beta c^2/4 \\ &\geq \beta^2 c^2, \end{aligned}$$

for sufficiently small β, and the algorithm terminates for c satisfying $\|\psi\|_2^2 < \beta c^2 \leq 4\|\psi\|_2^2$, if it hasn't already terminated for larger c. (Note that, in the first iteration, $\|\psi\|_2^2 \leq \|\mathbf{f}\|_2^2 \leq M^2 = \beta^2 c^2/4 < \beta c^2$, so there are such c.) In any case, the output satisfies $X/(1+\beta) \geq 0.5\|\mathbf{f}\|_2^2$.

The number of iterations is at most $\log_{1+\beta}(2M/\beta)$, to reduce c from the initial value of $2M/\beta$ to 1, through reductions by the factor $1/(1+\beta)$. The number k of samples at each step depends only on $\beta > 0$, which is independent of N and M. Finally, note that we can reuse the same sample for each iteration. If we want the overall probability of success to be at least $3/4$, then the probability of failure at each iteration needs to be at most $O(\beta/\log(M/\beta))$, *i.e.*, $1/4$ divided by the number of iterations. To achieve this, we need $O(\log\log(M))$ samples. ∎

The probability of success can be boosted from "significant" (*i.e.*, 3/4) to "high" (*i.e.*, $1-p$, for any desired p), by taking a median of $O(\log(1/p))$ repetitions and appealing to the Chernoff bound, as usual.

Figure 2: Filter functions $\hat{\mathbf{g}}_k$, for $N = 96$, and $k = 0, 4$, and 5. The region pass_0 is highlighted.



Lemma 8 *There is a sampling algorithm, A, with time and sample complexity $\log(M)\log^{O(1)}(N)$, such that, on input a 98% pure vector $\mathbf{f}$ of length N, A identifies the frequency ω' of the biggest Fourier coefficient of $\mathbf{f}$.*

Proof: Observe that, for some k, $0 \leq k < 16$, $\omega' \in \mathrm{pass}_k$; without loss of generality, assume $k = 0$. Now, consider the function $\mathbf{f} \star \mathbf{g}_0$. Since $\omega' \in \mathrm{pass}_0$, we have $|\widehat{\mathbf{f} \star \mathbf{g}_0}(\omega')| \geq 0.99|\hat{\mathbf{f}}(\omega')|$. Thus the pure frequency $\widehat{\mathbf{f} \star \mathbf{g}_0}(\omega')\psi_{\omega'}$ satisfies

$$\begin{aligned} |\widehat{\mathbf{f} \star \mathbf{g}_0}(\omega')|^2 &\geq (0.99)^2\|\psi\|_2^2 \\ &\geq (0.99)^2(0.98)\|\mathbf{f}\|_2^2 \\ &= (0.99)^2(0.98)\|\hat{\mathbf{f}}\|_2^2 \\ &\geq (0.95)\|\hat{\mathbf{f}}\|_2^2 \\ &\geq (0.95)\|\hat{\mathbf{f}}\hat{\mathbf{g}}_0\|_2^2 \\ &= (0.95)\|\mathbf{f} \star \mathbf{g}_0\|_2^2 \end{aligned}$$

It follows that, if we use Lemma 3 to estimate $\|\mathbf{f} \star \mathbf{g}_0\|_2^2$, the estimate will be at least

$$\begin{aligned} (0.5)\|\mathbf{f} \star \mathbf{g}_0\|_2^2 &\geq (0.5)|\widehat{\mathbf{f} \star \mathbf{g}_0}(\omega')|^2 \\ &\geq (0.5)(0.99)^2(0.98)\|\mathbf{f}\|_2^2 \\ &\geq (0.48)\|\mathbf{f}\|_2^2. \end{aligned}$$

On the other hand, now consider $f \star \mathbf{g}_4$. Note that

$$\begin{aligned} |\widehat{\mathbf{f} \star \mathbf{g}}_4(\omega')| &= |\hat{f}(\omega')|\widehat{\mathbf{g}}_4(\omega') \\ &\leq |\hat{f}(\omega')|(1 + \cos(2\pi(\omega'/N - 4/16)))/2 \\ &\leq |\hat{f}(\omega')|(1 + \cos(2\pi(1/32 - 4/16)))/2, \\ &\qquad \text{since } \cos(2\pi(\omega/N - 4/16)))/2 \text{ increases on } \mathrm{pass}_0 \ni \omega' \\ &\leq 0.6|\hat{f}(\omega')|, \\ &\leq 0.6\|\mathbf{f}\|_2. \end{aligned}$$

Also,

$$\begin{aligned} \|\widehat{\mathbf{f} \star \mathbf{g}}_4\|_2^2 - |\widehat{\mathbf{f} \star \mathbf{g}}_4(\omega')|^2 &\leq \|\rho\|_2^2 \\ &\leq 0.02\|\mathbf{f}\|_2^2. \end{aligned}$$

Thus $\|\mathbf{f} \star \mathbf{g}_4\|_2^2 \leq (0.6)^2\|\mathbf{f}\|_2^2 + 0.02\|\mathbf{f}\|_2^2 = 0.38\|\mathbf{f}\|_2^2$. It follows that if we use Lemma 3 to estimate $\|\mathbf{f} \star \mathbf{g}_4\|_2^2$, the result will be at most $(0.38)\|\mathbf{f}\|_2^2 \leq (0.48)\|\mathbf{f}\|_2^2$, which is a lower bound for the estimate of $\|\mathbf{f} \star \mathbf{g}_0\|_2^2$. Similarly, for all $4 \leq k \leq 12$, if we use Lemma 3 to estimate $\|\mathbf{f} \star \mathbf{g}_k\|_2^2$, then, since $\mathbf{g}_k(\omega') \leq (1 + \cos(2\pi(1/32 - 4/16)))/2$, the result will be less than the estimate of $\|\mathbf{f} \star \mathbf{g}_0\|_2^2$. In general, if $\omega' \in \mathrm{pass}_{k'}$ for k' not necessarily 0, we can reliably determine that $\omega \notin \mathrm{pass}_k$, for $|k - k'| \geq 4$, *i.e.*, we can rule out 9/16 of the possibilities opposite the region $\mathrm{pass}_{k'}$ where ω' lies. Thus, for $0 \leq k' < 16$ and $|k - k'| \geq 4$, we compare $\|\mathbf{f} \star \mathbf{g}_{k'}\|_2^2$ with $\|\mathbf{f} \star \mathbf{g}_k\|_2^2$. If there is some such k with $\|\mathbf{f} \star \mathbf{g}_k\|_2^2$ apparently larger than $\|\mathbf{f} \star \mathbf{g}_{k'}\|_2^2$, then we conclude $\omega' \notin \mathrm{pass}_{k'}$; otherwise, possibly, $\omega' \in \mathrm{pass}_{k'}$. By the above argument, we can always eliminate 9 consecutive pass regions out of the 16, leaving a cyclic interval of length at most $7N/16$.

In the sequel, it will be convenient to express the situation as follows. Let P denote a cyclic interval of odd size at most $7N/16 + 1$ that includes all possibilities for ω'. Let b_1 denote the center

of P. Then the spectrum of $f_1(t) = e^{-2\pi i b_1 t/N} f(t)$ is a shift of the spectrum of $\mathbf{f}$ by $-b_1$. Thus we know b_1, we know that $\omega' - b_1$ is the biggest frequency of $e^{2\pi i b_1 t/N} f(t)$, and we know $\omega' - b_1$ is in the range $-(7N/32+1)$ to $+(7N/32+1)$. We will now seek $\omega' - b_1$.

Intuitively, we dilate the spectrum of $\mathbf{f}_1$ by 2, which can be accomplished in the time domain by dilating $\mathbf{f}_1$ by $1/2$. Thus the interval of length just less than $N/2$ known to contain $\omega' - b_1$ is dilated to the alternate positions in an interval of length just less than N. We then rule out a cyclic interval of length at least $N/2$ in the dilated spectrum, leaving at most an interval of length $N/2$ in the dilated spectrum. We now undo the dilation, getting an interval of length just less than $N/4$, centered at some known b_2, as the possibilities for $\omega' - b_1$. That is, we've learned the equivalent of the second most significant bit of ω'. We repeat this to learn the other bits of ω'. We now proceed formally. Most of the work below is technical, to do arithmetic simultaneously over the integers and over the integers mod N.

In the following, we assume N is an odd prime; later, we give some discussion about how to proceed for general N. We represent the numbers mod N by the representatives $\{-(N-1)/2, \ldots, -1, 0, 1, \ldots, (N-1)/2\}$. We say "$b$ is a multiple of 2^j" to mean "the representative of b is a multiple of 2^j over the integers."

We will make a series of tests, for $j = 0, 1, \ldots, O(\log(N))$. We maintain the following invariant. After test j (that is, after making $j+1$ tests, each of which roughly cuts the space of possibilities in half), we will have a number b_j such that $\omega' - b_j$ is the biggest coefficient in $\mathbf{f}_j = R_{b_j,0} f(t)$ and $2^j(\omega' - b_j)$ is a multiple of 2^j in the range $[-((7/32)N + 2^j), +((7/32)N + 2^j)]$. We now show how to proceed, preserving the invariant. We assume that the set of possibilities for $\omega' - b_j$ contains more than $\log^2(N)$ elements; otherwise, check each element using Lemma 2. Thus we can assume that $2^{j+1}((7/32)N/2^j + 1) = 7N/16 + 2^{j+1} < (N-1)/2 - 2^{j+1}$. Consider the signal $R_{\theta,\sigma}\mathbf{f}_j$, where σ is invertible mod N and t/σ is computed modulo N. We are interested in $R_{0,2^{j+1}}\mathbf{f}_j$; we have $\widehat{R_{0,2^{j+1}}\mathbf{f}_j}(\omega) = \hat{\mathbf{f}}_j(2^{j+1}\omega)$. As above, for some k', $2^{j+1}(\omega' - b_j) \in \text{pass}_{k'}$, and we can determine that $2^{j+1}(\omega' - b_j) \notin \text{pass}_k$, for $|k - k'| \geq 4$, leaving an interval of length at most $7N/16$ for $2^{j+1}(\omega' - b_j)$. Observe that

$$\{2^{j+1}\omega : 2^j\omega \in [-((7/32)N + 2^j), +((7/32)N + 2^j)]\}$$

consists of all multiples of 2^{j+1} in the range $[-(7N/16 + 2^{j+1}), +(7N/16 + 2^{j+1})]$, which we assume is contained in $[-((N-1)/2 - 2^{j+1}), +((N-1)/2 - 2^{j+1})]$. As above, let P be a cyclic interval of length at most $7N/16 + 2^{j+1}$ that contains all the possibilities for $2^{j+1}(\omega' - b_j)$ and contains an odd number of multiples of 2^{j+1}. Let c be the middle multiple of 2^{j+1} in P. Then the possibilities for $2^{j+1}(\omega' - b_j) - c$ are among the multiples of 2^{j+1} in the range $[-((7/32)N + 2^j), +((7/32)N + 2^j)]$. Since $c \in [(N-1)/2, (N-1)/2]$ is a multiple of 2^{j+1} over the integers, the division $c/2^{j+1}$ is the same over the integers and modulo N. It follows that the possibilities for $2^{j+1}(\omega' - b_j - c/2^{j+1})$ are contained in the interval $[-((7/32)N + 2^{j+1}), +((7/32)N + 2^{j+1})]$. Put $b_{j+1} = b_j - c/2^{j+1}$. Thus the invariant is preserved, *i.e.*, $\omega' - b_{j+1}$, the biggest frequency of $R_{b_{j+1},0} f(t)$, is in the interval $[-((7/32)N + 2^{j+1}), +((7/32)N + 2^{j+1})]$.

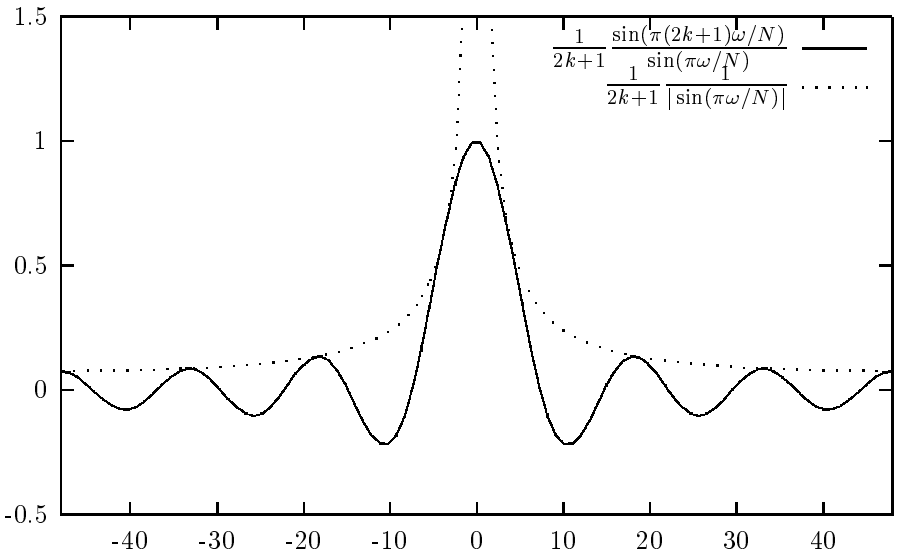
Eventually, for $j \leq O(\log(N))$, we learn $\omega' - b_j$ precisely, and, since we know b_j, we learn ω'.

∎

Note that our algorithm adapts to the signal values (for example, the b_j's depend on the signal values). But the choices of samples to the original signal do not depend on the signal values. For example, to sample $f_1(t) = e^{-2\pi i b_1 t/N} f(t)$ at t, just sample f at t and then multiply by $e^{-2\pi i b_1 t/N}$.

Above we assumed that N is prime, so that 2 is relatively prime to N. We then used the transform $R_{0,2^j}$. In general, we just need some number b to take the role of 2, such that b is relatively prime to N and $b \leq \log^{O(1)}(N)$. In particular, if N is a power of 2, we could use $b = 3$. The necessary changes to the above algorithm are straightforward, and omitted. Finally, the prime number theorem states that the $\log(N)$'th prime is approximately $\log(N)\log\log(N)$. Since N is less than the product of the first $\log(N)$ primes, some prime less than $\log(N)\log\log(N)$ does not divide N. The least b not dividing N can be found in time $\log^{O(1)}(N)$ by linear search. It follows that the above techniques hold for all N.

Figure 3: Filter function $\hat{\mathbf{h}}_k$ based on Fejér kernel, for $N = 96$ and $k = 6$, together with envelope.



Lemma 12 *Given signal* $\mathbf{a}$ *and number* η *we can create* $2k+1$ *new signals,* $\mathbf{f}_0, \ldots, \mathbf{f}_{2k}$*, such that:*

- *For each* ω' *such that* $|\hat{a}(\omega')|^2 \geq \eta\|\mathbf{a}\|_2^2$*, there exists a* j *such that* $|\hat{f}_j(\omega')|^2 \geq 0.98\|\mathbf{f}_j\|_2^2$.
- *Each* $\mathbf{f}_j$ *can be sampled by sampling non-adaptively from* $\mathbf{a}$ *in* $O(k)$ *places.*
- k *is small,* i.e.*,* $k \leq O(1/\eta)$.

Proof: Pick θ and σ at random, with σ invertible. Let $k \leq O(1/\eta)$ be sufficiently large. Then consider the signal

$$\mathbf{f}_j = (e^{2\pi ijt/(2k+1)}\mathbf{h}_k) \star R_{\theta,\sigma}\mathbf{a},$$

for $0 \leq j < 2k+1$. Semantically, $\hat{\mathbf{f}}_j$ is formed by starting with $\hat{\mathbf{a}}$, performing a pairwise-independent permutation (in the frequency domain), then multiplying pointwise by a phase shift of $\hat{\mathbf{h}}_k$ by $jN/(2k+1)$.

One can sample a chosen point of $R_{\theta,\sigma}a$ by sampling a single chosen point from a. It follows that one can sample a chosen point from $f_j = (e^{2\pi ijt/(2k+1)}\mathbf{h}_k) \star R_{\theta,\sigma}a$ by sampling $|\mathrm{supp}(\mathbf{h}_k)| = 2k+1$ chosen points from a (in arithmetic progression).

Fix j such that $(j-1/2)N/(2k+1) \leq \sigma\omega' + \theta < (j+1/2)N/(2k+1)$; we show that $|\hat{f}_j(\sigma\omega'+\theta)|^2 \geq 0.98\|\mathbf{f}_j\|_2^2$. First, observe that

$$\begin{aligned} |\hat{f}_j(\sigma\omega'+\theta)|^2 &\geq (2/\pi)^2|\hat{a}(\omega')|^2 \\ &\geq (\eta/4)\|\hat{\mathbf{a}}\|_2^2, \end{aligned}$$

since $|\hat{h}_k(\sigma\omega'+\theta)| \geq (2/\pi)$. We now show that $\|\hat{\mathbf{f}}_j\chi_{[0,N)\setminus\sigma\omega'+\theta}\|_2^2 \leq (\eta/200)\|\hat{a}\|_2^2$. We have

$$\begin{aligned} E_{\theta,\sigma}\left[\left\|\hat{\mathbf{f}}_j\chi_{[0,N)\setminus\sigma\omega'+\theta}\right\|_2^2 \;\middle|\; (j-1/2)N/(2k+1) \leq \sigma\omega'+\theta < (j+1/2)N/(2k+1)\right] \\ &= E_{\theta,\sigma}\left[\left\|\hat{\mathbf{f}}_j\chi_{[0,N)\setminus\sigma\omega'+\theta}\right\|_2^2\right], \quad \text{by pairwise independence} \\ &\leq E_{\theta,\sigma}[\|\hat{\mathbf{f}}_j\|_2^2] \\ &= E_{\theta,\sigma}\left[\sum_\omega |\hat{f}_j(\omega)|^2\right] \\ &= \sum_\omega E_{\theta,\sigma}[|\hat{f}_j(\omega)|^2] \\ &= \sum_\beta \frac{1}{N}\sum_\gamma |\hat{h}_k(\gamma)|^2|\hat{a}(\beta)|^2, \quad \text{by change of variables} \\ &= \frac{1}{N}\|\mathbf{a}\|_2^2\|\hat{\mathbf{h}}_k\|_2^2 \\ &= \frac{\|\mathbf{a}\|_2^2}{2k+1}. \end{aligned}$$

By Markov's inequality,

$$\Pr_{\theta,\sigma}\left[\left\|\hat{\mathbf{f}}_j\chi_{[0,N)\setminus\sigma\omega'+\theta}\right\|_2^2 > \frac{4\|\mathbf{a}\|_2^2}{2k+1} \;\middle|\; jN/(2k+1) \leq \sigma\omega'+\theta < (j+1)N/(2k+1)\right] \leq 1/4,$$

so

$$\Pr_{\theta,\sigma}\left[\left\|\hat{\mathbf{f}}_j\chi_{[0,N)\setminus\sigma\omega'+\theta}\right\|_2^2 > (\eta/200)\|\hat{\mathbf{a}}\|_2^2 \;\middle|\; jN/(2k+1) \leq \sigma\omega'+\theta < (j+1)N/(2k+1)\right] \leq 1/4,$$

for $2k+1 = 800/\eta$.

As usual, the success probability $3/4$ can be boosted to probability $1-p$ with cost factor $O(\log(1/p))$. In this case, repeat the experiment $O(\log(1/p))$ times with independent randomness, and take the union of all $O(k\log(1/p))$ candidates for ω'. The probability that ω is not among them is the product of the probabilities, $(1/4)^{\log(1/p)} = p$.

We can therefore make the probability that ω' is among the candidates at least $1-\eta/4$. Since there are at most $1/\eta$ possible ω''s, the probability that *all* ω''s are among the candidates is at least $3/4$. In turn, this probability can also be boosted, if desired. ∎

In case N is not prime, the above proof can be modified to work. First, choose σ at random but relatively prime to N, so that σ is still invertible. The permutation $\omega \mapsto \pi(\omega) = \sigma\omega + \theta$ is not pairwise independent; for example, if N is a power of 2, then $0 \mapsto \theta$ and $N/4 \mapsto N/4+\theta$ or $N/4 \mapsto 3N/4+\theta$. For each q dividing N, we need to sum the contribution to $E_{\theta,\sigma}\left[\left\|\hat{\mathbf{f}}_j \chi_{[0,N)\setminus\sigma\omega'+\theta}\right\|_2^2\right]$ due to ω with $\gcd(\omega' - \omega, N) = q$. As above, one can show that the expected contribution due to all such $\omega \neq \omega'$ is $\frac{1}{2k+1}$ of the total. By summing over q, the result follows. We omit the details.

Theorem 13 *Fix a signal* $\mathbf{a}$ *with integer-valued elements. Suppose, for all representations* $\mathbf{r}'$ *of at most* B *terms, we can, with cost* $1/\eta^{O(1)}$*,*

- *estimate* $\widehat{\mathbf{a}-\mathbf{r}'}(\omega)$ *as* $\widehat{\tilde{\mathbf{a}-\mathbf{r}'}}(\omega)$ *with* $|\widehat{\mathbf{a}-\mathbf{r}'}(\omega) - \widehat{\tilde{\mathbf{a}-\mathbf{r}'}}(\omega)|^2 \leq \eta\|\mathbf{a}\|_2^2$
- *output a list of at most* $1/\eta^{O(1)}$ *frequencies that contains all frequencies* ω *such that* $|\widehat{\mathbf{a}-\mathbf{r}'}(\omega)|^2 \geq \eta\|\mathbf{a}-\mathbf{r}'\|_2^2$.

Then we can, on input B *and* ϵ*, with cost* $(B\log(N)\log(M)/\epsilon)^{O(1)}$ *output a* B*-term representation* $\mathbf{r}$ *with sum-square-error* $\|\mathbf{a}-\mathbf{r}\|_2^2 \leq (1+\epsilon)\|\mathbf{a}-\mathbf{r}_{\text{opt}}\|_2^2$*, where* $\mathbf{r}_{\text{opt}}$ *is the* B*-term representation for* $\mathbf{a}$ *with the least sum-square-error.*

Proof: We use the greedy algorithm of Figure 4. This is the classic greedy pursuit algorithm, except:

- When searching for a new coefficient for our representation, we cannot find the biggest coefficient, only a near-biggest. Since (in this variant of greedy pursuit) we have no facility to eject a wrongly-chosen coefficient, we need to argue that each coefficient we take is acceptable.
- Our algorithm revisits frequencies, so it cannot halt after B steps. Furthermore, unlike a classic algorithm that can measure its progress and can halt when no further improvement is possible, our algorithm in general continues even after no further progress is possible. We need to show that potential extraneous rounds of greedy pursuit performed by our algorithm don't worsen things by much.

Each of these is straightforward to check. For completeness, we present the entire greedy pursuit algorithm.

The algorithm clearly halts, quickly, and outputs a representation of at most B terms. We now argue that the representation has sufficiently small error. Let δ denote the error of the best B-term representation (with optimal coefficients).

We show that the following invariant is maintained:

- At line LOOPING, $\mathbf{a}$ has an approximate representation of B terms extending S', with error at most

$$\left(1 + \frac{\epsilon|S'|}{2B}\right)\delta.$$

Figure 4: Greedy algorithm for Fourier approximation to signal a

---

SAMPLING:

$T_0 \leftarrow (B\log(N)\log(M/\delta)/\epsilon)^{O(1)}$ random points in $[0, N)$

$T \leftarrow \emptyset$ // set of sample indices

for($t \in T_0$)

{

$\sigma \in_R \mathbf{Z}_N^*$ // σ random invertible scaling factor for isolation

for($j \leftarrow 0; j < \log(N); j \leftarrow j + 1$) // different scales for group testing

for($k \leftarrow 0; k < (B/\epsilon)^O(1); k \leftarrow k + 1$) // building the Fejér kernel

$T \leftarrow T \cup \{t - 2^j + k\sigma, t + k\sigma, t + 2^j + k\sigma\}$ // three points in $\mathrm{supp}(1 + \cos())$˘

}

$\alpha \leftarrow \mathbf{a}\chi_T$ // $\mathbf{a}$ on sample T of $[0, N)$

COMPUTING REPRESENTATION:

$S' \leftarrow \emptyset$ // set of $\leq B$ basis vectors

$\mathbf{r}' \leftarrow 0$ // representation

$J \leftarrow (B\log(N)\log(M/\delta)/\epsilon)^{O(1)}$

for($j \leftarrow 0; j < J; j \leftarrow j + 1$)

{

$\Lambda \leftarrow \text{identify}\left(\alpha, T_0, \frac{\epsilon}{2B}\right)$ // $\Lambda \supseteq \left\{\omega : |c_\omega|^2 > \frac{\epsilon}{2B}\|\mathbf{a} - \mathbf{r}'\|_2^2\right\}$, $|\Lambda| \leq (B\log(N)/\epsilon)^{O(1)}$

if $|S'| == B$

$\Lambda \leftarrow \Lambda \cap S'$

if $\Lambda == \emptyset$

break; // go to REPORT:

LOOPING:

for($\omega \in \Lambda$)

$\tilde{c}_\omega \leftarrow \text{estimate}\left(\omega, \alpha, T_0, \frac{\epsilon}{24j^2B^2}\right)$ // $\tilde{c}_\omega = \langle \mathbf{a} - \mathbf{r}', \psi_\omega \rangle \pm \frac{\epsilon}{3 \cdot 24j^2B^2}\|\mathbf{a} - \mathbf{r}'\|_2$

// so $|\tilde{c}_\omega|^2 = |\langle \mathbf{a} - \mathbf{r}', \psi_\omega \rangle|^2 \pm \frac{\epsilon}{24j^2B^2}\|\mathbf{a} - \mathbf{r}'\|_2^2$

$\omega' \leftarrow \text{argmax}_{\omega \in \Lambda}(\tilde{c}_\omega)$

$S' \leftarrow S' \cup \{\omega'\}$

$\mathbf{r}' \leftarrow \mathbf{r}' + c_{\omega'}\psi_{\omega'}$ // formally—maintain the representation

$\alpha \leftarrow (\alpha - \tilde{c}_{\omega'}\psi_{\omega'})\,\chi_T$ // α has $(\mathbf{a} - \mathbf{r}')\chi_\Sigma$

}

REPORT:

Output $\mathbf{r}'$

By "extension" of S', we mean a representation $\mathbf{r}''$ over frequencies in $S'' \supseteq S'$. An extension of S' might be the current representation $\mathbf{r}'$ on S' itself, might involve new terms, or might have better approximations to the terms in $\mathbf{r}'$.

By hypothesis, the invariant is true the first time line LOOPING is executed. Suppose execution is at Line LOOPING at an arbitrary time, with the invariant holding. We now show that if, at Line LOOPING, S' is extendible, then $S' \cup \{\omega'\}$ is extendible. This is clearly true if $\omega' \in S'$, so we assume that $\omega' \notin S'$, so that $\Lambda \leftarrow \Lambda \cap S'$ is not executed, and ω' is the argmax of the originally identified set.

First, suppose $\delta < \frac{1}{6B}\|\mathbf{a} - \mathbf{r}'\|_2^2$. Then, since some B-term extension of $\mathbf{r}'$ has error at most $(1+\epsilon)\delta$, it follows that the largest coefficient has energy at least

$$\begin{aligned}\frac{\|\mathbf{a} - \mathbf{r}'\|_2^2 - (1+\epsilon)\delta}{B} &\geq \frac{\|\mathbf{a} - \mathbf{r}'\|_2^2 - 2B\delta}{B} \\ &\geq \frac{2\|\mathbf{a} - \mathbf{r}'\|_2^2}{3B},\end{aligned}$$

and so appears on our list of candidates. Thus the frequency ω' whose coefficient appears largest by our estimation procedure has energy at least

$$\begin{aligned}\frac{2\|\mathbf{a} - \mathbf{r}'\|_2^2}{3B} - \frac{2\epsilon}{24j^2B^2}\|\mathbf{a} - \mathbf{r}'\|_2^2 &\geq \frac{2\|\mathbf{a} - \mathbf{r}'\|_2^2}{3B} - \frac{1}{3B}\|\mathbf{a} - \mathbf{r}'\|_2^2 \\ &\geq \frac{\|\mathbf{a} - \mathbf{r}'\|_2^2}{3B} \\ &> 2\delta \\ &\geq (1+\epsilon)\delta,\end{aligned}$$

for $\epsilon < 1$, so ω' is in any extension with error at most $(1+\epsilon)\delta$.

Now, suppose $\delta \geq \frac{1}{6B}\|\mathbf{a} - \mathbf{r}'\|_2^2$. Let ω^* be the frequency whose coefficient is actually largest, so ω^*, if unique, is in any optimal extension; even if ω^* is not unique, it can go into any optimal extension. We have

$$\begin{aligned}|c_{\omega'}|^2 &\geq |\tilde{c}_{\omega'}|^2 - \frac{\epsilon}{24j^2B^2}\|\mathbf{a} - \mathbf{r}'\|_2^2 \\ &\geq |\tilde{c}_{\omega^*}|^2 - \frac{\epsilon}{24j^2B^2}\|\mathbf{a} - \mathbf{r}'\|_2^2 \\ &\geq |c_{\omega^*}|^2 - \frac{\epsilon}{12j^2B^2}\|\mathbf{a} - \mathbf{r}'\|_2^2 \\ &\geq |c_{\omega^*}|^2 - \frac{\epsilon}{2B}\delta.\end{aligned}$$

Thus, if we choose ω' instead of ω^*, at worst, we displace ω^* by ω' in an optimal extension. It follows that the error of the best extension to $S' \cup \{\omega'\}$ is at most the error of the best extension of S' plus $|c_{\omega^*}|^2 - |c_{\omega'}|^2$, *i.e.*, at most

$$\begin{aligned}\delta\left(1 + \frac{\epsilon|S'|}{2B}\right) + |c_{\omega^*}|^2 - |c_{\omega'}|^2 &\leq \delta\left(1 + \frac{\epsilon|S'|}{2B}\right) + \frac{\epsilon}{2B}\delta \\ &\leq \delta\left(1 + \frac{\epsilon|S' \cup \{j\}|}{2B}\right).\end{aligned}$$

It follows that the invariant is preserved. We now consider the correctness of the output. First we show that, for some iteration $j' < J$, the representation is good enough; next we argue that subsequent iterations cannot worsen the representation by much. Thus, however we exit the loop, the final representation has acceptable error.

Suppose $\|\mathbf{a} - \mathbf{r}'\|_2^2 > (1 + 7\epsilon/8)\delta$. Then, since an extension has error at most $(1 + \epsilon/2)\delta$, it follows that some optimal coefficient c_{ω^*} with $|S' \cup \{\omega^*\}| \leq B$ has energy at least $(3\epsilon/(8B))\|\mathbf{a} - \mathbf{r}'\|_2^2 \geq (\epsilon/(4B))\|\mathbf{a} - \mathbf{r}'\|_2^2$, so is identified. Thus

$$\begin{aligned}
|c_{\omega'}|^2 &\geq |\tilde{c}_{\omega'}|^2 - (\epsilon/(24j^2B^2))\|\mathbf{a} - \mathbf{r}'\|_2^2 \\
&\geq |\tilde{c}_{\omega^*}|^2 - (\epsilon/(24j^2B^2))\|\mathbf{a} - \mathbf{r}'\|_2^2 \\
&\geq |c_{\omega^*}|^2 - (\epsilon/(12j^2B^2))\|\mathbf{a} - \mathbf{r}'\|_2^2 \\
&\geq (3\epsilon/(8B))\|\mathbf{a} - \mathbf{r}'\|_2^2 - (\epsilon/(12j^2B^2))\|\mathbf{a} - \mathbf{r}'\|_2^2 \\
&\geq (7\epsilon/(24B))\|\mathbf{a} - \mathbf{r}'\|_2^2.
\end{aligned}$$

It follows that the new representation, $\mathbf{r}' + \tilde{c}_{\omega'}\psi_{\omega'}$, has error

$$\begin{aligned}
\|\mathbf{a} - (\mathbf{r}' + \tilde{c}_{\omega'}\psi_{\omega'})\|_2^2 &= \|\mathbf{a} - \mathbf{r}'\|_2^2 - |c_{\omega'}|^2 + |\tilde{c}_{\omega'} - c_{\omega'}|^2 \\
&\leq \|\mathbf{a} - \mathbf{r}'\|_2^2 - (7\epsilon/(24B))\|\mathbf{a} - \mathbf{r}'\|_2^2 + (\epsilon/(24j^2B^2))\|\mathbf{a} - \mathbf{r}'\|_2^2 \\
&\leq (1 - \epsilon/(4B))\|\mathbf{a} - \mathbf{r}'\|_2^2.
\end{aligned}$$

Thus, after $O(B\log(M/\delta)/\epsilon)$ iterations, the error of $\mathbf{r}'$ has been reduced from $\|\mathbf{a}\|_2^2$ by the factor

$$(1 - \epsilon/(4B))^{O(B\log(M)/\epsilon)} \leq 1/M,$$

a contradiction. It follows that, for some $j' < J$, after j' iterations, $\|\mathbf{a} - \mathbf{r}'\|_2^2 \leq (1 + 7\epsilon/8)\delta$.

Now consider the representation after the j''th iteration. The list of identified coefficients will still be short, but is otherwise arbitrary. Thus we choose some arbitrary frequency ω', estimate $c_{\omega'}$ up to $(\epsilon/(24j^2B^2))\|\mathbf{a} - \mathbf{r}'\|_2^2$ as $\tilde{c}_{\omega'}$, and add $\tilde{c}_{\omega'}\psi_{\omega'}$ to our growing representation. It follows that the new representation has error at most $(1 + \epsilon/(24j^2B^2))\|\mathbf{a} - \mathbf{r}'\|_2^2$. Whenever we exit, the representation at that time has error at most

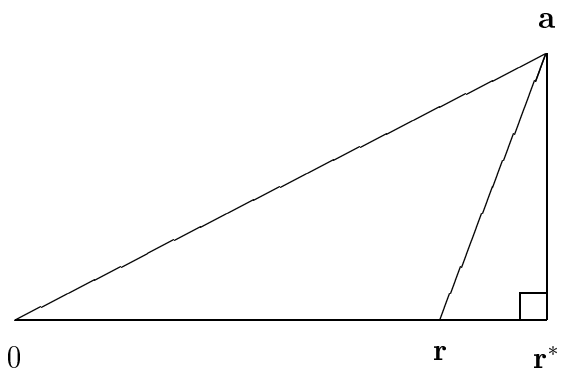
$$\begin{aligned}
(1 + 7/8\epsilon)\delta\prod_{j=1}^{\infty}(1 + \epsilon/(24j^2B^2)) &\leq (1 + 7/8\epsilon)\delta\prod_{j=1}^{\infty}e^{\epsilon/(24j^2B^2)} \\
&= (1 + 7/8\epsilon)\delta e^{\frac{\epsilon}{24}\sum_{j=1}^{\infty}1/j^2} \\
&\leq (1 + 7/8\epsilon)\delta e^{\epsilon/14} \\
&\leq (1 + 7/8\epsilon)\delta(1 + \epsilon/10)) \\
&\leq (1 + \epsilon)\delta,
\end{aligned}$$

if ϵ is sufficiently small.

Thus the final representation has error at most $(1 + \epsilon)\delta$. ∎

Lemma 14 *Suppose* $\mathbf{r}$ *is a representation for* a *such that* $\|\mathbf{a} - \mathbf{r}\|_2^2 \leq (1 + \epsilon)\|\mathbf{a} - \mathbf{r}_{\text{opt}}\|_2^2$. *Then* $\|\mathbf{a} - \mathbf{r}\|_2^2 = \|\mathbf{a}\|_2^2 - \|\mathbf{r}\|_2^2 \pm 4\sqrt{\epsilon}\|\mathbf{a}\|_2^2$.

Figure 5: Assessing the quality of $\mathbf{r}$.



Proof: Let $\mathbf{r}^*$ denote the real multiple of $\mathbf{r}$ that minimizes $\|\mathbf{a}-\mathbf{r}\|_2^2$. Thus the $\mathbf{a}$-$\mathbf{r}^*$-0 angle is a right angle. (See Figure 5.) By near-optimality of $\mathbf{r}$ and because $\mathbf{r}^*$ is a B-term representation,

$$\begin{aligned}\|\mathbf{a}-\mathbf{r}^*\|_2^2+\|\mathbf{r}^*-\mathbf{r}\|_2^2 &= \|\mathbf{a}-\mathbf{r}\|_2^2\\ &\le (1+\epsilon)\|\mathbf{a}-\mathbf{r}_{\rm opt}\|_2^2\\ &\le (1+\epsilon)\|\mathbf{a}-\mathbf{r}^*\|_2^2,\end{aligned}$$

so that

$$\begin{aligned}\|\mathbf{r}^*-\mathbf{r}\|_2^2 &\le \epsilon\|\mathbf{a}-\mathbf{r}^*\|_2^2\\ &\le \epsilon\|\mathbf{a}-\mathbf{r}\|_2^2\\ &\le \epsilon(1+\epsilon)\|\mathbf{a}-\mathbf{r}_{\rm opt}\|_2^2\\ &\le \epsilon(1+\epsilon)\|\mathbf{a}\|_2^2.\end{aligned}$$

Also,

$$\begin{aligned}\big|\|\mathbf{r}\|_2^2-\|\mathbf{r}^*\|_2^2\big| &= \big(\|\mathbf{r}\|_2+\|\mathbf{r}^*\|_2\big)\big|\|\mathbf{r}\|_2-\|\mathbf{r}^*\|_2\big|\\ &\le 3\|\mathbf{r}-\mathbf{r}^*\|_2\|\mathbf{a}\|_2, \quad \text{since } \|\mathbf{r}^*\|_2^2\le\|\mathbf{a}\|_2^2 \text{ and } \|\mathbf{r}\|_2^2\le(1+\epsilon)\|\mathbf{a}\|_2^2\le 2\|\mathbf{a}\|_2^2\\ &\le 3\sqrt{\epsilon(1+\epsilon)}\|\mathbf{a}\|_2^2.\end{aligned}$$

Thus

$$\begin{aligned}\|\mathbf{a}-\mathbf{r}\|_2^2 &= \|\mathbf{a}-\mathbf{r}^*\|_2^2+\|\mathbf{r}^*-\mathbf{r}\|_2^2\\ &= \|\mathbf{a}\|_2^2-\|\mathbf{r}^*\|_2^2+\|\mathbf{r}^*-\mathbf{r}\|_2^2\\ &= \|\mathbf{a}\|_2^2-\|\mathbf{r}\|_2^2+(\|\mathbf{r}\|_2^2-\|\mathbf{r}^*\|_2^2)+\|\mathbf{r}^*-\mathbf{r}\|_2^2\\ &= \|\mathbf{a}\|_2^2-\|\mathbf{r}\|_2^2\pm 3\sqrt{\epsilon(1+\epsilon)}\|\mathbf{a}\|_2^2\pm\epsilon(1+\epsilon)\|\mathbf{a}\|_2^2\\ &= \|\mathbf{a}\|_2^2-\|\mathbf{r}\|_2^2\pm 4\sqrt{\epsilon}\|\mathbf{a}\|_2^2,\end{aligned}$$

for ϵ sufficiently small. ∎