GEOMETRIC APPROACH TO ERROR CORRECTING CODES AND RECONSTRUCTION OF SIGNALS

MARK RUDELSON AND ROMAN VERSHYNIN

Abstract. We develop an approach through geometric functional analysis to error correcting codes and to reconstruction of signals from few linear measurements. An error correcting code encodes an n-letter word x into an m-letter word y in such a way that x can be decoded correctly when any r letters of y are corrupted. We show that most linear orthogonal transformations $Q : \mathbb{R}^n \to \mathbb{R}^m$ form efficient and robust robust error correcting codes over reals. The decoder (which corrects the corrupted components of y) is the metric projection onto the range of Q in the ℓ_1 norm. This yields robust error correcting codes over reals (and over alphabets of polynomial size), with a Gilbert-Varshamov type bound, and with quadratic time encoders and polynomial time decoders. An equivalent problem arises in signal processing: how to reconstruct a signal that belongs to a small class from few linear measurements? We prove that for most sets of Gaussian measurements, all signals of small support can be exactly reconstructed by the L_1 norm minimization. This is an improvement of recent results of Donoho and of Candes and Tao. An equivalent problem in combinatorial geometry is the existence of a symmetric polytope with fixed number of facets and maximal number of lower-dimensional facets. We prove that most sections of a cube form such polytopes. Our work thus belongs to a common ground of coding theory, signal processing, combinatorial geometry and geometric functional analysis. Our argument, which is based on concentration of measure and improving Lipschitzness by random projections, may be of independent interest in geometric functional analysis.

1. Error correcting codes and transform coding

Error correcting codes are used in modern technology to protect information from errors. Information is formed by finite words over some alphabet $\mathbb{F}$. An encoder transforms an n-letter word x into an m-letter word y with $m > n$. The decoder must be able to recover x correctly when up to r letters of y are corrupted in any way. Such an encoder-decoder pair is called an (n, m, r)-*error correcting code*.

Development of algorithmically efficient error correcing codes has been attracting attention of engineers, computer scientists and applied mathematicians for past five decades. Known constructions involve deep algebraic and combinatorial methods, see [26], [32], [33]. This paper develops an approach to error correcting codes from

Date: February 14, 2005.

2000 *Mathematics Subject Classification.* 46B07, 94B75, 68P30, 52B05.

The first author is partially supported by the NSF grant DMS 0245380. The second author is an Alfred P. Sloan Research Fellow He was also partially supported by the NSF grant DMS 0401032 and by the Miller Scholarship from the University of Missouri-Columbia.

the viewpoint of geometric functional analysis (asymptotic convex geometry). It thus belongs to a common ground of coding theory, signal processing, combinatorial geometry and geometric functional analysis. Our argument, outlined in Section 3, may be of independent interest in geometric functional analysis.

Our main focus will be on words over the alphabet $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$. In applications, these words may be formed of the coefficients of some signal (such as image or audio) with respect to some basis or overcomplete system (Fourier, wavelet, etc.) Finite alphabets will be discussed in Section 5.

The simplest and most natural way to encode a vector $x \in \mathbb{R}^n$ into a vector $y \in \mathbb{R}^m$ is of course a linear transform

$$y = Qx \tag{1.1}$$

where Q is given by an $m \times n$ matrix. Elementary linear algebra tells us that if $m \geq n + 2r$ and the range of Q is generic[1] then x can be recovered from y even if r coordinates of y are corrupted. This gives an (n, m, r)-error correcting code. However, the decoder for this code has a huge computational complexity, as it involves a search through all r-element subsets of the components of y. Then the problem is:

> *How to reconstruct a vector y in an n-dimensional subspace Y of $\mathbb{R}^m$ from a vector $y' \in \mathbb{R}^m$ that differs from y in at most r coordinates?*

What complicates this problem is the arbitrary magnitude of errors in each corrupted component of y', in contrast to what happens over finite alphabets such as $\mathbb{F} = \{0, 1\}$.

A traditional and simple approach to denoising y', used in applications such as signal processing, is the mean least square (MLS) minimization. One hopes that y is well approximated by a solution to the minimization problem

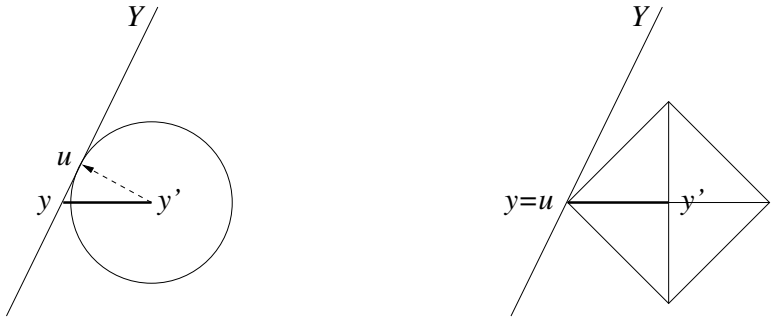
$$\min_{u \in Y} \|u - y'\|_2 \tag{MLS}$$

where $\|x\|_2^2 = \sum_i |x_i|^2$. The solution to (MLS) is simply the orthogonal projection of y' onto Y. This of course can not recover y exactly, and even the approximation is typically poor since we have no control of the magnitude of the errors in the corrupted coordinates. A promising alternative approach is the *Basis Pursuit* (BP). We simply replace the 1-norm by the 2-norm and expect y to be the *exact* and unique solution to the minimization problem

$$\min_{u \in Y} \|u - y'\|_1 \tag{BP}$$

where $\|x\|_1 = \sum_i |x_i|$. Thus a solution to (BP) is the metric projection of y' onto Y with respect to the 1-norm. (BP) be cast as a Linear Programming problem, and can be attacked with a variety of methods, such as the classical simplex method or more recent interior point methods that yield polynomial time algorithms [4].

[1] that is, in general position with respect to all subspaces $\mathbb{R}^I$, $|I| = r$



(MLS) (BP)

The potential of Basis Pursuit for exact reconstruction is illustrated by the following heuristics, essentially due to [13]. The solution u to (MLS) is the contact point where the smallest Euclidean ball centered at y' meets the subspace Y. That contact point is in general different from y. The situation is much better in (BP): typically the solution coincides with y. The solution u to (BP) is the contact point where the smallest octahedron centered at y' (the ball with respect to the 1-norm) meets Y. Because the vector $y - y'$ lies in a low-dimensional coordinate subspace, the octahedron has a wedge at y. Thus, many subspaces Y through y will miss the octahedron of radius $y - y'$ (as opposed to the Euclidean ball). This forces the solution u to (BP), which is the contact point of the octahedron, to coincide with y.

The idea of using the 1-norm instead of the 2-norm for better data recovery has been explored since mid-seventies in various applied areas, in particular geophysics and statistics (early history can be found in [36]). With the subsequent development of fast interior point methods in Linear Programming, (BP) turned into an effectively solvable problem, and was put forward more recently by Donoho and his collaborators, triggering massive experimental and theoretical work [4, 17, 18, 19, 14, 25, 34, 35, 36, 13, 10, 11, 15, 16, 7, 6, 8].

The main result of this paper validates the Basis Pursuit method for most subspaces Y under an asymptotically sharp condition on m, n, r. We thus prove that *the Basis Pursuit yields exact reconstruction for most subspaces Y* in the Grassmanian. The randomness is with respect to the normalized Haar measure on the Grassmanian $G_{m,n}$ of n-dimensional subspaces of $\mathbb{R}^m$. Positive absolute constants will be denoted throughout the paper by $C, c, C_1, \ldots$.

Theorem 1.1. *Let m, n and $r < cm$ be positive integers such that*

$$m = n + R, \quad \text{where } R \geq Cr \log(m/r). \tag{1.2}$$

Then a random n-dimensional subspace Y in $\mathbb{R}^m$ satisfies the following with probability at least $1 - e^{-cR}$. Let $y \in Y$ be an unknown vector, and we are given a vector y' in $\mathbb{R}^m$ that differs from y on at most r coordinates. Then y can be exactly reconstructed from y' as the solution to the minimization problem (BP).

In an equivalent form, this theorem is an improvement of recent results of Donoho [10] and of Candes and Tao [8], see Theorem 2.1 below.

1.1. **Error correcting codes.** Theorem 1.1 implies a natural (n, m, r)-error correcting code over $\mathbb{R}$. The encoder (1.1) is given by an $m \times n$ random orthogonal matrix[2] Q. Its range Y is a random n-dimensional subspace in $\mathbb{R}^m$. The decoder takes a corrupted vector y', solves (BP) and outputs $Q^T u = Q^{-1} u$. Theorem 1.1 states that this encoder-decored pair is an (n, m, r)-error correcting code with exponentially good probability $\geq 1 - e^{-cR}$, provided the assumption (1.2) holds.

Assumption (1.2) meets, up to an absolute constant, the *Gilbert-Varshamov bound* which is fundamental in coding theory (see [26]): $n/m \geq 1 - H(Cr/n)$, where $H(x)$ is the entropy function. The encoder runs in quadratic time in the size n of the input, the decoder runs in polynomial time.

1.2. **Sharpness.** The sufficient condition (1.2) is sharp up to an absolute constant C (see Section 5) and is only slightly stronger than the necessary condition $m \geq n + 2r$. The ratio $\varepsilon = r/m$ in (1.2) is the number of errors per letter in the noisy communication channel that maps y to y'. Thus ε should be considered as a quality of the channel, which is independent of the message. Thus (1.2) is equivalent to

$$m \geq \Big(1 + C\varepsilon \log \frac{1}{\varepsilon}\Big) n.$$

1.3. **Robustness.** An natural feature of our error correction code is its *robustness*. Simple linear algebra yields that the solution to (BP) is stable with respect to the 1-norm – in the same way as the solution to (MLS) is stable with respect to the 2-norm, see [8]. Such robustness allows in particular quantization of the messages. This immediately yields robust and polynomial-time error correcting codes for finite alphabets, which asymptotically meet the Gilbert-Varshamov bound, see Section 5.

1.4. **Transform coding.** In the signal processing, the linear codes (1.1) are known as *transform codes*. The general paradigm about transform codes is that the redundancies in the coefficients of y that come from the excess of the dimension $m > n$ should guarantee a stability of the signal with respect to noise, quantization, erasures, etc. This is confirmed by an extensive experimental and some theoretical work, see e.g. [9, 21, 22, 24, 23, 27, 3, 5] and the bibliography contained therein. Theorem 1.1 states that *most orthogonal transform codes are good error-correcting codes*.

Acknowledgement. This work has started when the second author was visiting University of Missouri-Columbia as a Miller Visiting Scholar. He is grateful to the UMC for the hospitality.

When this paper was completed, we have learned about a new independent and similar project of E.Candes and T.Tao.

[2] one can view it as the first n rows of a random matrix from $O(m)$ equipped with the normalized Haar measure.

2. Reconstruction of signals from linear measurements.

The heuristic idea that guides the Statistical Learning Theory is that *a function f from a small class should be determined by few linear measurements.* Linear measurements are generally given by some linear functionals X_k in the dual space, which are fixed (in particular are independent of f). Most common measurements are point evaluation functionals; the problem there is to interpolate f between known values while keeping f in the known (small) class. When the evaluation points are chosen at random, this becomes the 'proper learning' problem of the Statistical Learning Theory (see [31]).

We shall however be interested in general linear measurements. The proposal to learn f from general linear measurements (*'sensing'*) has been originated recently from a criticism of the current methodology of signal compression. Most of real life signals, such as images and sounds, seem to belong to small classes. This is because they carry much of unwanted information that can be discarded with almost no perceptual loss, which makes such signals easily compressible. Donoho [12] then questions the conventional scheme of signal processing, where the whole signal must be first acquired (together with lots of unwanted information) and only then be compressed (throwing away the unwanted part). Instead, can one *directly acquire* ('sense') the essential part of the signal, via few linear measurements? Similar issues are raised in [8]. We shall operate under the assumption that some technology allows us to take linear measurements in certain fixed 'directions' X_k.

We will assume that our signal f is discrete, so we view it as a vector in $\mathbb{R}^m$. Suppose we can take linear measurements $\langle f, X_k\rangle$ with some fixed vectors $X_1, X_2, \dots, X_R$ in $\mathbb{R}^m$. Assuming that f belongs to a small class, how many measurements R are needed to reconstruct f? And even when we prove that R measurements do determine f (uniquely or approximately), the algorithmic issue remains unsettled: how can one reconstruct f from these measurements?

The previous section suggests to reconstruct f as a solution to the Basis Pursuit minimization problem

$$\min \|g\|_1 \quad \text{subsect to} \quad \langle g, X_k\rangle = \langle f, X_k\rangle, \quad k = 1, \dots, R. \tag{BP$'$}$$

For the Basis Pursuit to work, the vectors X_k must be in a good position with respect to all coordinate subspaces $\mathbb{R}^I$, $|I| \le r$. A typical choice for such vectors would be the independent standard Gaussian vectors[3] X_k.

2.1. Functions with small support.

In the class of functions with small support, one can hope for exact reconstruction. Candes and Tao [8] have indeed proved that every *fixed* function f with support $|\mathrm{supp} f| \le r$ can indeed be recovered by (BP$'$), correctly with the polynomial probability $1 - m^{-\mathrm{const}}$, from the $R = Cr \log m$ Gaussian measurements. However, the polynomial probability is clearly not sufficient to deduce that there is *one* set vectors X_k that can be used to reconstruct all functions f of small support.

[3] All the components of X_k are independent standard Gaussian random variables.

The following equivalent form of Theorem 1.1 does yield a uniform exact reconstruction. It provides us with *one set* of linear measurements from from which we can effectively reconstruct *every* signal of small support.

Theorem 2.1 (Uniform Exact Reconstruction)**.** *Let m, $r < cm$ and R be positive integers satisfying $R \geq Cr\log(m/r)$. The independent standard Gaussian vectors X_k in $\mathbb{R}^m$ satisfy the following with probability at least $1 - e^{-cR}$. Let $f \in \mathbb{R}^m$ be an unknown function of small support, $|\mathrm{supp} f| \leq r$, and we are given R measurements $\langle f, X_k\rangle$. Then f can be exactly reconstructed from these measurements as a solution to the Basis Pursuit problem (BP$'$).*

This theorem gives uniformity in Candes-Tao result [8], improves the polynomial probability to an exponential probability, and improves upon the number R of measurements (which was $R \geq Cr\log m$ in [8]). Donoho [12] proved a weaker form of Theorem 2.1 with R/r bounded below by some function of m/r.

Proof. Write $g = f - u$ for some $u \in \mathbb{R}^m$. Then (BP$'$) reads as

$$\min \|u - f\|_1 \ \text{ subsect to } \ \langle u, X_k\rangle = 0, \quad k = 1, \dots, R. \tag{2.1}$$

The constraints here define a random $(n = m - R)$-dimensional subspace Y of $\mathbb{R}^m$. Now apply Theorem 1.1 with $y = 0$ and $y' = f$. It states that the unique solution to (2.1) is $u = 0$. Therefore, the unique solution to (BP$'$) is f. ∎

2.2. **Compressible functions.** In a larger class of compressible functions [12], we can only hope for an approximate reconstruction. This is a class of functions f that are well compressible by a known orthogonal transform, such as Fourier or wavelet. This means that the coefficients of f with respect to a certain known orthogonal basis have a power decay. By applying an appropriate rotation, we can assume that this basis is the canonical basis of $\mathbb{R}^m$, thus f satisfies

$$f^*(s) \leq s^{-1/p}, \quad s = 1, \dots, m \tag{2.2}$$

where f^* denotes a nonincreasing rearrangement of f. Many natural signals are compressible for some $0 < p < 1$, such as smooth signals and signals with bounded variations (see [8]), in particular most photographic images. Theorem 2.1 implies, by the argument of [8], that functions compressible in some basis can be approximately reconstructed from few fixed linear measurements. This is an improvement of a result of Donoho [12].

Corollary 2.2 (Uniform Approximate Reconstruction)**.** *Let m and r be positive integers. The independent standard Gaussian vectors X_k in $\mathbb{R}^m$ satisfy the following with probability at least $1 - e^{-cR}$. Assume that an unknown function $f \in \mathbb{R}^m$ satisfies either (2.2) for some $0 < p < 1$ or $\|f\|_1 \leq 1$ for $p = 1$. Suppose that we are given R measurements $\langle f, X_k\rangle$. Then f can be approximately reconstructed from these measurements: a unique solution g to the Basis Pursuit problem (BP$'$) satisfies*

$$\|f - g\|_2 \leq C_p \Big(\frac{\log(m/R)}{R}\Big)^{\frac{1}{p} - \frac{1}{2}}$$

where C_p depends on p only.

Corollary 2.2 was proved by Donoho [12] under an additional assumption that $m \sim CR^\alpha$ for some $\alpha > 1$. Notice that in this case $\log(m/R) \sim \log m$. Now this assumption is removed. Candes and Tao [8] proved Corollary 2.2 without the uniformity in f due to a weaker (polynomial) probability. Finally, Corollary 2.2 also improves upon the approximation error (there is now the ratio m/r instead of m in the logarithm).

3. Counting low-dimensional facets of polytopes.

Theorem 1.1 turns out to be equivaent to a problem of counting lower-dimensional facets of polytopes. Let B_1^m denote the unit ball with respect to the 1-norm; it is sometimes called the unit octahedron. The polar body is the unit cube $B_\infty^m = [-1,1]^m$. The conclusion of Theorem 1.1 is then equivalent to the following statement: the affine subspace $z+Y$ is tangent to the unit octahedron at point z, where $z = y' - y$. This should happen for all z from the coordinate subspaces $\mathbb{R}^I$ with $|I| = r$. By the duality, this means that the subspace $Y^\perp$ intersects all $(m-r)$-dimensional facets of the unit cube. The section of the cube by the subspace $Y^\perp$ forms an origin-symmetric polytope of dimension R and with $2m$ facets.

Our problem can thus be stated as a problem of counting lower-dimensional facets of polytopes.

Consider an R-dimensional origin symmetric polytope with $2m$ facets. How many $(R-r)$-dimensional facets can it have?

Clearly[4], no more than $2^r\binom{m}{r}$. Does there exist a polytope with that many facets? Our ability to construct such a polytope is equivalent to the existence of the efficient error correcting code. Indeed, looking at the canonical realization of such a polytope as a section of the unit cube by a subspace $Y^\perp$, we see that $Y^\perp$ intersects all the $(m-r)$-dimensional facets of the cube. Thus Y satisfies the conclusion of Theorem 1.1. We can thus state Theorem 1.1 in the following form:

Theorem 3.1. *There exists an R-dimensional symmetric polytope with m facets and with the maximal number of $(R-r)$-dimensional facets (which is $2^r\binom{m}{r}$), provided $R \geq Cr\log(m/r)$. A random section of the cube forms such a polytope with probability $1-e^{-cR}$.*

So, how can we prove that a random subspace $Y^\perp$ indeed intersects all the $(m-r)$-dimensional facets of the cube? It is enough to show that $Y^\perp$ intersects one such fixed facet with exponential probability (bigger than $1-2^{-r}\binom{m}{r}^{-1}$). The main difficulty here is that the concentration of measure technique can not be readily applied. This is because the ∞-norm defined by the unit cube (more precisely, by its facet) has a bad Lipschitz constant. To improve the Lipschitzness, we first project the facet onto a random subspace (within its affine span); the random subspace parallel to which we project is taken from the random directions that form $Y^\perp$. This creates a big Euclidean ball inside the projected facet; here we shall use the full strength of the estimate of Garnaev and Gluskin [20] on Euclidean projections of a cube. The

[4]Any such facet is the intersection of some r facets of the polytope of full dimension $R-1$; there are m facets to choose from, each coming with its opposite by the symmetry.

existence of the Euclidean ball inside a body creates the needed Lipschitzness, so we can now use the concentration of measure tecnique.

The rest of the paper is organized as follows. In Section 4 we prove Theorem 1.1. In Section 5 we discuss some optimality and robustness of the Basis Pursuit with applications to error correcting codes over finite alphabets.

4. Proof

We shall use the following standard notations throughout the proof. The p-norm ($1 \le p < \infty$) on $\mathbb{R}^m$ is defined by $\|x\|_p^p = \sum_i |x_i|^p$, and for $p = \infty$ it is $\|x\|_\infty = \max_i |x_i|$. The unit ball with respect to the p-norm on $\mathbb{R}^n$ is denoted by B_p^m. When the p-norm is considered on a coordinate subspace $\mathbb{R}^I$, $I \subset \{1, \dots, m\}$, the corresponding unit ball is denoted by B_p^I.

The unit Euclidean sphere in a subspace E is denoted by $S(E)$. The normalized rotational invariant Lebesgue measure on $S(E)$ is denoted by σ_E. The orthogonal projection in onto a subspace E is denoted by P_E. The standard Gaussian measure on E (with the identity covariance matrix) is denoted by γ_H. When $E = \mathbb{R}^d$, we write σ_{d-1} for σ_E and γ_d for γ_E.

4.1. **Duality.** We begin the proof of Theorem 1.1 with a typical duality argument, leading to the same reformulation of the problem as in [8]. We claim that the conclusion of Theorem 1.1 follows from (and is actually equivalent to) the following separation condition:

$$(z + Y) \cap \text{ interior}\,(B_1^m) = \emptyset \quad \text{for all} \quad z \in \bigcup_{|I|=r} B_1^I. \tag{4.1}$$

Indeed, suppose (4.1) holds. We apply it for

$$z := \frac{y - y'}{\|y - y'\|_1}$$

noting that $z \in \bigcup_{|I|=r} B_1^I$ holds, because y and y' differ in at most r coordinates. By (4.1),

$$(z + v) \cap \text{ interior}\,(B_1^m) = \emptyset \quad \text{for all } v \in Y$$

which implies

$$\|z + v\|_1 \ge 1 \quad \text{for all } v \in Y.$$

Let $u \in Y$ be arbitrary. Using the inequality above for $v := \frac{u-y}{\|u-y\|_1}$, we conclude that

$$\|u - y\|_1 \ge \|y - y'\|_1 \quad \text{for all } u \in Y.$$

This proves that y is indeed a solution to (BP). The solution to (BP) is unique with probability 1 in the Grassmanian. This follows from a direct dimension argument, see e.g. [8].

By Hahn-Banach theorem, the separation condition 4.1 is equivalent to the following: for every $z \in \bigcup_{|I|=r} \text{boundary}\, B_1^I$ there exists $w = w(z) \in Y^\perp$ such that

$$\langle w, z \rangle = \sup_{x \in B_1^m} \langle w, x \rangle = \|w\|_\infty.$$

This holds if and only if the components of w satisfy

$$\begin{cases} w_j = \operatorname{sign}(z_j) \ \text{ for } j \in I, \\ |w_j| \le 1 \ \text{ for } j \in I^c. \end{cases} \tag{4.2}$$

The set of vectors w in $\mathbb{R}^m$ that satisfy (4.2) form a $(m-r)$-dimensional facet of the unit cube B_∞^m. Then with $E := Y^\perp$ we can say that the conclusion of Theorem 1.1 is equivalent to the following:

> *A random R-dimensional subspace E in $\mathbb{R}^m$ intersects all the $(m-r)$-dimensional facets of the unit cube with probability at least $1 - e^{-cR}$.*

It will be enough to show that E intersects *one fixed* facet with the probability $1 - e^{-cR}$. Indeed, since the total number of the facets is $N = 2^r \binom{m}{r}$, the probability that E misses some facet would be at most $Ne^{-cR} \le e^{-c_1 R}$ with an appropriate choice of the absolute constant in (1.2).

4.2. **Realizing a random subspace.** We are to show that a random R-dimensional subspace E intersects one fixed $(m-r)$-dimensional facet of the unit cube B_∞^m with high probability. Without loss of generality, we can assume that our facet is

$$F = \{(w_1, \dots, w_{m-r}, 1, \dots, 1), \ \text{ all } |w_j| \le 1\},$$

whose center is

$$\theta = (\underbrace{0, \dots, 0}_{m-r}, 1, \dots, 1).$$

The probability we are interested in is

$$P := \operatorname{Prob}\{E \cap F \ne \emptyset\}.$$

We shall restrict our attention to the linear span of F,

$$\operatorname{lin}(F) = \{(w_1, \dots, w_{m-r}, t, \dots, t), \ \text{ all } w_j \in \mathbb{R},\, t \in \mathbb{R}\},$$

and even to its the affine span of F,

$$\operatorname{aff}(F) = \{(w_1, \dots, w_{m-r}, 1, \dots, 1), \ \text{ all } w_j \in \mathbb{R}\}.$$

Only the random affine subspace $E \cap \operatorname{aff}(F)$ matters for us, because

$$P = \operatorname{Prob}\Big\{(E \cap \operatorname{aff}(F)) \cap F \ne \emptyset\Big\}.$$

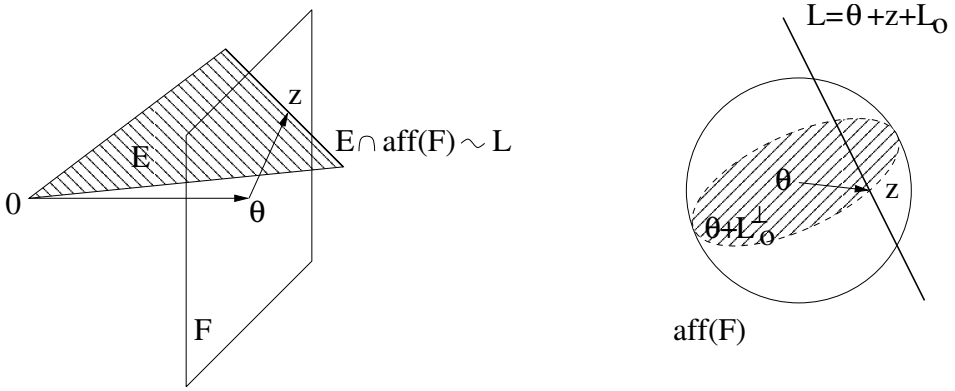
The dimension of that affine subspace is almost surely

$$l := \dim(E \cap \operatorname{aff}(F)) = R - r.$$

We can realize the random affine subspace $E \cap \operatorname{aff}(F)$ (or rather a random subspace with the same law) by the following algorithm:

(1) Select a random variable D with the same law as $\operatorname{dist}(\theta, E \cap \operatorname{aff}(F))$.
(2) Select a random subspace L_0 in the Grassmanian $G_{m-r,l}$. It will realize the "direction" of $E \cap \operatorname{aff}(F)$ in $\operatorname{aff}(F)$.

(3) Select a random point z on the Euclidean sphere $D \cdot S(L_0^\perp)$ of radius D, according to the uniform distribution on the sphere. Here $L_0^\perp$ is the orthogonal complement of L_0 in $\mathbb{R}^{m-r}$. The vector z will realize the distance from the affine subspace $E \cap \mathrm{aff}(F)$ to the center θ of F.
(4) Set $L = \theta + z + L_0$. Thus the random affine subspace L has the same law as $E \cap \mathrm{aff}(F)$.



Hence

$$P = \mathrm{Prob}\{L \cap F \neq \emptyset\} = \mathrm{Prob}\{(z + L_0) \cap B_\infty^{m-r} \neq \emptyset\} = \mathrm{Prob}\{z \in P_{L_0^\perp} B_\infty^{m-r}\}.$$

$H := L_0^\perp$ is a random subspace in $G_{m-r,m-r-l} = G_{m-r,m-R}$. By the rotational invariance of $z \in D \cdot S(H)$,

$$P = \int_{\mathbb{R}^+} \int_{G_{m-r,m-R}} \sigma_H(D^{-1} P_H B_\infty^{m-r})\, d\nu(H)\, d\mu(D) \tag{4.3}$$

where ν is the normalized Haar measure on $G_{m-r,m-R}$ and μ is the law of D. We shall bound P in two steps:

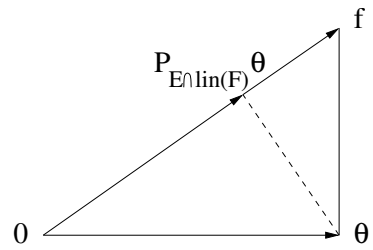
(1) Prove that the distance D is small with high probability;
(2) Prove that a suitable multiple of the random projection $P_H B_\infty^{m-r}$ has an almost full Gaussian (thus also spherical) measure.

4.3. **The distance D from the center of the facet to a random subspace.** We shall first relate D, the distance to the affine subspace $E \cap \mathrm{aff}(F)$, to the distance to the linear subspace $E \cap \mathrm{lin}(F)$. Equivalently, we compute the length of the projection onto $E \cap \mathrm{lin}(F)$.

Lemma 4.1.

$$\|P_{E \cap \mathrm{lin}(F)} \theta\|_2 = \sqrt{\frac{r}{r + D^2}}\, \|\theta\|_2.$$

Proof. Let f be the multiple of the vector $P_{E \cap \mathrm{lin}(F)} \theta$ such that $f - \theta$ is orthogonal to θ. Such a multiple exists and is unique, as this is a two-dimensional problem.



Then $f \in E \cap \mathrm{aff}(F)$. Notice that $D = \|f - \theta\|_2$. By the similarity of the triangles with the vertices $(0, \theta, P_{E\cap\mathrm{lin}(F)}\theta)$ and $(0, f, \theta)$, we conclude that

$$\|P_{E\cap\mathrm{lin}(F)}\theta\|_2 = \frac{r}{\sqrt{r+D^2}} = \sqrt{\frac{r}{r+D^2}}\ \|\theta\|_2$$

because $\|\theta\|_2 = \sqrt{r}$. This completes the proof. ∎

The length of the projection of a fixed vector onto a random subspace in Lemma 4.1 is well known. The asymptotically sharp estimate was computed by S. Artstein [1], but we will be satisfied with a much weaker elementary estimate, see e.g. [30] 15.2.2.

Lemma 4.2. *Let $\theta \in \mathbb{R}^{d-1}$ and let G be a random subspace in $G_{d,k}$. Then*

$$\mathrm{Prob}\Big\{c\sqrt{\frac{k}{d}}\ \|\theta\|_2 \le \|P_G\theta\|_2 \le C\sqrt{\frac{k}{d}}\ \|\theta\|_2\Big\} \ge 1 - 2e^{-ck}.$$

We apply this lemma for $G = E \cap \mathrm{lin}(F)$, which is a random subspace in the Grassmanian of $(l+1)$-dimensional subspaces of $\mathrm{lin}(F)$. Since $\dim \mathrm{lin}(F) = m-r+1$, we have

$$\mathrm{Prob}\Big\{\|P_{E\cap\mathrm{lin}(F)}\theta\|_2 \ge c\sqrt{\frac{l+1}{m-r+1}}\ \|\theta\|_2\Big\} \ge 1 - 2e^{-cl}.$$

Together with Lemma 4.1 this gives

$$\mathrm{Prob}\Big\{D \le c\sqrt{m-r}\sqrt{\frac{r}{l}}\Big\} \ge 1 - 2e^{-cl}. \tag{4.4}$$

Note that $\sqrt{m-r}$ is the radius of the Euclidean ball circumscribed on the facet F. The statement $D \le \sqrt{m-r}$ would only tell us that the random subspace E intersects the circumscribed ball, not yet the facet itself. The ratio r/l in (4.4) will be chosen logarithmically small, which will force E intersect also the facet F.

4.4. **Gaussian measure of random projections of the cube.** By (4.3) and (4.4),

$$P \ge \int_{G_{m-r,m-R}} \sigma_H\Big(\frac{c}{\sqrt{m-r}}\sqrt{\frac{l}{r}}\,P_H B_\infty^{m-r}\Big)\,d\nu(H) - 2e^{-cl}.$$

We can replace the spherical measure σ_H by the Gaussian measure γ_H via a simple lemma:

Lemma 4.3. *Let K be a star-shaped set in $\mathbb{R}^d$. Then*

$$\gamma_d(c\sqrt{d}\cdot K) - e^{-d} \le \sigma_{d-1}(K) \le \gamma_d(C\sqrt{d}\cdot K)\cdot(1+e^{-d}).$$

Proof. Passing to polar coordinates, by the rotational invariance of the Gaussian measure we see that there exists a probability measure μ on $\mathbb{R}^+$ so that the Gaussian measure of every set A can be computed as $\int_{\mathbb{R}^+} \sigma^t(A)\, d\mu(t)$, where σ^t denotes the normalized Lebesgue measure on the Euclidean sphere of radius t in $\mathbb{R}^d$. Since K is star-shaped, $\sigma^t(K)$ is a non-increasing function of t. Hence

$$\gamma_d(K) \geq \int_0^{C\sqrt{d}} \sigma^t(K)\, d\mu(t) \geq \sigma^{C\sqrt{d}}(K) \cdot \gamma_d(C\sqrt{d}B_2^d)$$

and

$$\gamma_d(K) \leq \int_0^{c\sqrt{d}} d\mu(t) + \sigma^{c\sqrt{d}}(K) \int_{c\sqrt{d}}^{\infty} d\mu(t) \leq \gamma_d(c\sqrt{d} \cdot B_2^d) + \sigma^{c\sqrt{d}}(K).$$

The classical large deviation inequalities imply $\gamma_d(c\sqrt{d} \cdot B_2^d) \leq e^{-d}$ and $\gamma_d(C\sqrt{d}B_2^d) \geq 1 - e^{-d}/2$. Using the above argument for $c\sqrt{d} \cdot K$, we conclude that $\gamma_d(c\sqrt{d} \cdot K) \leq e^{-d} + \sigma_{d-1}(K)$ and $\gamma_d(C\sqrt{d} \cdot K) \geq \sigma_{d-1}(K) \cdot (1 - e^{-d}/2)$. ∎

Using Lemma 4.3 in the space H of dimension $d = m - R$, we obtain

$$P \geq \int_{G_{m-r,m-R}} \gamma_H\Big(c\sqrt{\frac{m-R}{m-r}}\sqrt{\frac{l}{r}}\, P_H B_\infty^{m-r}\Big)\, d\nu(H) - 2e^{-cl} - e^{m-R}.$$

By choosing the absolute constant c in the assumption $r < cm$ appropriately small, we can assume that $2r < R < m/2$. Thus

$$P \geq \int_{G_{m-r,m-R}} \gamma_H\Big(c\sqrt{\frac{R}{r}}\, P_H B_\infty^{m-r}\Big)\, d\nu(H) - 2e^{-cR}. \tag{4.5}$$

We now compute the Gaussian measure of random projections of the cube.

Proposition 4.4. *Let H be a random subspace in $G_{n,n-k}$, $k < n/2$. Then the inequality*

$$\gamma_H\Big(C\sqrt{\log\frac{n}{k}}\, P_H B_\infty^n\Big) \geq 1 - e^{-ck}$$

holds with probability at least $1 - e^{-ck}$ in the Grassmanian.

The proof of this estimate will follow from the concentration of Gaussian measure, combined with the existence of a big Euclidean ball inside a random projection of the cube.

Lemma 4.5 (Concentration of Gaussian measure)**.** *Let A be a measurable set in $\mathbb{R}^n$. Then for $\varepsilon > 0$,*

$$\gamma_n(A) \geq e^{-\varepsilon^2 n} \quad \textit{implies} \quad \gamma_n(A + C\varepsilon\sqrt{n}B_2^n) \geq 1 - e^{-\varepsilon^2 n}.$$

With the stronger assumption $\gamma(A) \geq 1/2$, this lemma is the classical concentration inequality, see [28] 1.1. The fact that the concentration holds also for exponentially small sets follows formally by a simple extension argument that was first noticed by D. Amir and V. Milman in [2], see [28] Lemma 1.1.

The optimal result on random projections of the cube is due to Garnaev and Gluskin [20].

Theorem 4.6 (Euclidean projections of the cube [20])**.** *Let H be a random subspace in $G_{n,n-k}$, where $k = \alpha n < n/2$. Then with probability at least $1 - e^{-ck}$ in the Grassmanian, we have*

$$c(\alpha)\, P_H(\sqrt{n}B_2^n) \subseteq P_H(B_\infty^n) \subseteq P_H(\sqrt{n}B_2^n)$$

where

$$c(\alpha) = c\sqrt{\frac{\alpha}{\log(1/\alpha)}}.$$

Proof of Proposition 4.4. Let $g_1, g_2, \dots$ be independent standard Gaussian random variables. Then for a suitable positive absolute constant c and for every $0 < \varepsilon < 1/2$,

$$\gamma_n\Big(C\sqrt{\log\frac{1}{\varepsilon}}\, B_\infty^n\Big) = \mathrm{Prob}\Big\{\max_{1\le j\le n} |g_i| \le C\sqrt{\log\frac{1}{\varepsilon}}\Big\} \ge (1-\varepsilon^2/10)^n \ge e^{-\varepsilon^2 n}.$$

Since for every measurable set A and every subspace H one has $\gamma_H(P_H A) \ge \gamma(A)$, we conclude that

$$\gamma_H\Big(C\sqrt{\log\frac{1}{\varepsilon}}\, P_H B_\infty^n\Big) \ge e^{-\varepsilon^2 n} \quad \text{for } 0 < \varepsilon < 1/2.$$

Then by Lemma 4.5,

$$\gamma_H\Big(C\sqrt{\log\frac{1}{\varepsilon}}\, P_H B_\infty^n + C\varepsilon\sqrt{n}\, P_H B_2^n\Big) \ge 1 - e^{-\varepsilon^2 n} \quad \text{for } 0 < \varepsilon < 1/2. \tag{4.6}$$

Theorem 4.6 tells us that for a random subspace H, if $\varepsilon = c\sqrt{\alpha} = c\sqrt{k/n}$, then Euclidean ball is absorbed by the projection of the cube in (4.6):

$$\varepsilon\sqrt{n}\, P_H B_2^n \subset C\sqrt{\log\frac{1}{\varepsilon}}\, P_H B_\infty^n.$$

Hence for a random subspace H and for ε as above we have

$$\gamma_H\Big(C\sqrt{\log\frac{1}{\varepsilon}}\, P_H B_\infty^n\Big) \ge 1 - e^{-\varepsilon^2 n},$$

which completes the proof. ∎

Coming back to (4.5), we shall use Lemma 4.4 for a random subspace H in the Grassmanian $G_{m-r,m-R}$. We conclude that if

$$c\sqrt{\frac{R}{r}} \ge C\sqrt{\log\frac{m-r}{R-r}}, \tag{4.7}$$

then with probability at least $1 - e^{-cR}$ in the Grassmanian,

$$\gamma_H\Big(c\sqrt{\frac{R}{r}}\, P_H B_\infty^{m-r}\Big) \ge 1 - e^{-cR}.$$

Since $\frac{m-r}{R-r} \le \frac{m}{r}$, the choice of R in (1.2) satisfies condition (4.7). Thus (4.5) implies

$$P \ge 1 - 3e^{-cR}.$$

This completes the proof. ∎

5. Optimality, robustness, finite alphabets

5.1. **Optimality.** The logarithmic term in Theorems 1.1 and 2.1 is necessary, at least in the case of small r. Indeed, combining formula (4.3) and Lemmas 4.1, 4.2, 4.3, we obtain

$$P \le \int_{G_{m-r,m-R}} \gamma_H\Big(c\sqrt{\frac{R}{r}}\, P_H B_\infty^{m-r}\Big)\, d\nu(H) + 2e^{-cR}. \tag{5.1}$$

To estimate the Gaussian measure we need the following

Lemma 5.1. *Let $x_1, \dots x_s$ be vectors in $\mathbb{R}^s$. Then*

$$\gamma_s\left(\sum_{j=1}^s [-x_j, x_j]\right) \le \gamma_s(M \cdot B_\infty^s),$$

where $M = \max_{j=1,\dots s} \|x_j\|_2$.

The sum in the Lemma is understood as the Minkowski sum of sets of vectors, $A + B = \{a + b \mid a \in A,\ b \in B\}$.

Proof. Let $F = \operatorname{span}(x_1, \dots x_{s-1})$ and let $V = F^\perp$. Let $v \in V$ be a unit vector. Set $Z = \sum_{j=1}^{s-1} [-x_j, x_j]$. Then

$$\begin{aligned}\gamma_s\Big(\sum_{j=1}^s [-x_j, x_j]\Big) &= \int_V \gamma_F\Big(\Big(\sum_{j=1}^s [-x_j, x_j] - tv\Big) \cap F\Big)\, d\gamma_V(t) \\ &= \int_{[-P_V x_s, P_V x_s]} \gamma_F(Z + tP_F x_s) d\gamma_V(t).\end{aligned}$$

By Anderson's Lemma (see [29]), $\gamma_F(Z + tP_F x_s) \le \gamma_F(Z)$. Thus,

$$\gamma_s\Big(\sum_{j=1}^s [-x_j, x_j]\Big) \le \gamma_V([-P_V x_s, P_V x_s]) \cdot \gamma_F(Z) \le \gamma_1([-M, M]) \cdot \gamma_F(Z).$$

The proof of the Lemma is completed by induction. ∎

The Gaussian measure of a projection of the cube can be estimated as follows.

Proposition 5.2. *Let H be any subspace in $G_{n,n-k}$, $k < n/2$. Then*

$$\gamma_H\Big(\frac{c}{\sqrt{k}}\sqrt{\log\frac{n}{k}}\, P_H B_\infty^n\Big) \le e^{-cn/k}. \tag{5.2}$$

Proof. Decompose I into the disjoint union of the sets $J_1, \dots J_{s+1}$, so that each of the sets $J_1, \dots J_s$ contains $k+1$ elements and $(k+1)s < n \le (k+1)(s+1)$. Let $1 \le j \le s$. Let $U_j = H \cap (P_H e_i,\ i \in \{1, \dots n\} \setminus J_j)^\perp$, where $e_1, \dots e_n$ is the standard basis of $\mathbb{R}^n$. Then U_j is a one-dimensional subspace of H. Set

$$x_j = \sum_{i \in J_j} \varepsilon_i P_H e_i,$$

where the signs $\varepsilon_i \in \{-1, 1\}$ are chosen to maximize $\|P_{U_j} x_j\|_2$. Let $E = \mathrm{span}(x_1, \dots x_{s-1})$. Since $P_{U_j} B_\infty^n = [-x_j, x_j]$, we get

$$P_H B_\infty^n \cap E = \sum_{j=1}^{s} [-x_j, x_j],$$

where the sum is understood in the sense of Minkowski addition. Since $\|P_{U_J}\| = 1$, $\|x_j\|_2 \le C\sqrt{k}$ and by Lemma 5.1,

$$\gamma_E \left(\frac{\bar{c}\sqrt{\log s}}{\sqrt{k}} \sum_{j=1}^{s} [-x_j, x_j] \right) \le \gamma_E(c' \sqrt{\log s} \cdot B_\infty^E) \le e^{-cs}$$

for some appropriately chosen constant $\bar{c}$. Finally, log-concavity of the Gaussian measure implies that for any convex symmetric body $K \subset H$

$$\gamma_H(K) \le \gamma_E(K \cap E).$$

■

Combining (5.1) and (5.2) we obtain $P \le 2e^{-cR}$, whenever $R \le c \log(m/r)$.

5.2. **Robustness and codes for finite alphabets.** Robustness is a well known property of the Basis Pursuit method. It states that the solution to (BP) is stable with respect to the 1-norm. Indeed, it is not hard to show that, once Theorem 1.1 holds, the unknown vector y in Theorem 1.1 can be approximately recovered from $y'' = y' + h$, where $h \in \mathbb{R}^m$ is any additional error vector of small 1-norm (see [8]). Namely, the solution u to the Basis Pursuit problem

$$\min_{u \in Y} \|u - y''\|_1$$

satisfies

$$\|u - y\|_1 \le 4\|h\|_1.$$

This implies a possibility of quantization of the coefficients in the process of encoding and yields *robust error correcting codes over alphabets of polynomial size, with a Gilbert-Varshamov type bound, and with quadratic time encoders and polynomial time decoders.*

The following is the (m, n, r)-error correcting code under the Gilbert-Varshamov type assumption (1.2), with input words x over the alphabet $\{1, \dots, p\}$ and the encoded words y over the alphabet $\{1, \dots, Cpn^{3/2}\}$.

The construction is the same as in (1.1); we just have to introduce quantization. The encoder takes $x \in \{1, \dots, p\}^n$, computes $y = Qx$ and outputs the $\hat{y}$ whose coefficients are the quantized coefficients of y with step $\frac{1}{10m}$. Then $\hat{y} \in \frac{1}{10m}\mathbb{Z}^m \cap$

$[-p\sqrt{m}, p\sqrt{m}]^m$, which by rescaling can be identified with $\{1, \dots, Cpn^{3/2}\}$ because we can assume that $m \le 2n$. The decoder takes $y' \in \frac{1}{10m}\mathbb{Z}^m$, finds solution u to (BP) with $Y = \text{range}(Q)$, inverts to $x' = Q^T u$ and outputs $\hat{x'}$ whose coefficients are the quantized coefficients of x' with step 1.

This is indeed an (m, n, r)-error correcting code. If y' differs from $\hat{y}$ on at most r coordinates, this and the condition $\|\hat{y} - y\|_1 \le \frac{1}{10}$ implies by the robustness that $\|u - y\|_1 \le 0.4$. Hence $\|x' - x\|_2 = \|Q^T(u - y)\|_2 = \|u - y\|_2 \le \|u - y\|_1 \le 0.4$. Thus $\hat{x'} = x$, so the decoder recovers x from y' correctly.

The robustness also implies a "continuity" of our error correcting codes. If the number of corrupted coordinates in the received message y' is bigger than r but is still a small fraction, then the (m, n, r)-error correcting code above can still recover y up to some small fraction of the coordinates.

We hope to return to consequences of our method, in particular to robustness and continuity of our codes and generally to codes over finite alphabets, in a separate publication.

References

[1] S. Artstein, *Proportional concentration phenomena on the sphere*, Israel J. Math. 132 (2002), 337–358

[2] D. Amir, V. D. Milman, *Unconditional and symmetric sets in n-dimensional normed spaces*, Israel J. Math. 37 (1980), 3–20

[3] B. Beferull-Lozano, A. Ortega, *Efficient quantization for overcomplete expansions in* $\mathbb{R}^n$, IEEE Trans. Inform. Theory 49 (2003), 129–150

[4] S. Chen, D. Donoho, M. Saunders, *Atomic decomposition by basis pursuit*, SIAM J. Sci. Comput. 20 (1998), no. 1, 33–61; reprinted in: SIAM Rev. 43 (2001), no. 1, 129–159

[5] P.G.Casazza, J.Kovacević, *Equal-norm tight frames with erasures. Frames*, Adv. Comput. Math. 18 (2003), 387–430

[6] E. Candes, J. Romberg, *Quantitative Robust Uncertainty Principles and Optimally Sparse Decompositions*, preprint

[7] E. Candes, J. Romberg, T. Tao, *Robust Uncertainty Principles: Exact Signal Reconstruction from Highly Incomplete Frequency Information*, preprint

[8] E. Candes, T. Tao, *Near Optimal Signal Recovery From Random Projections: Universal Encoding Strategies?*, preprint

[9] I.Daubechies, *Ten lectures on wavelets*, SIAM, Philadelphia, 1992

[10] D. Donoho, *For Most Large Underdetermined Systems of Linear Equations, the minimal* ℓ_1*-norm solution is also the sparsest solution*, preprint

[11] D. Donoho, *For Most Large Underdetermined Systems of Linear Equations, the minimal l1-norm near-solution approximates the sparsest near-solution*, preprint

[12] D. Donoho, *Compressed sensing*, preprint

[13] D. Donoho, M. Elad, V. Temlyakov, *Stable Recovery of Sparse Overcomplete Representations in the Presence of Noise*, preprint

[14] D. Donoho, M. Elad, *Optimally sparse representation in general (nonorthogonal) dictionaries via ell*$_1$ *minimization*, Proc. Natl. Acad. Sci. USA 100 (2003), 2197–2202

[15] D. Donoho, Y. Tsaig, *Extensions of compresed sensing*, preprint

[16] D. Donoho, Y. Tsaig, *Breakdown of Equivalence between the minimal l1-norm Solution and the Sparsest Solution*, preprint

[17] D. Donoho, X. Huo, *Uncertainty principles and ideal atomic decomposition*, IEEE Trans. Inform. Theory 47 (2001), 2845–2862

[18] M. Elad, A. Bruckstein, *A generalized uncertainty principle and sparse representation in pairs of bases*, IEEE Trans. Inform. Theory 48 (2002), 2558–2567

[19] A. Feuer, A. Nemirovski, *On sparse representation in pairs of bases*, IEEE Trans. Inform. Theory 49 (2003), 1579–1581

[20] A. Yu. Garnaev, E. D. Gluskin, *The widths of a Euclidean ball* (Russian), Dokl. Akad. Nauk SSSR 277 (1984), 1048–1052. English translation: Soviet Math. Dokl. 30 (1984), 200–204

[21] V.K.Goyal, *Theoretical Foundations of Transform Coding*, IEEE Signal Processing Magazine 18 (2001), no. 5, 9–21

[22] V.K.Goyal, *Multiple Description Coding: Compression Meets the Network*, IEEE Signal Processing Magazine 18 (2001), no. 5, 74–93

[23] V.K.Goyal, J.Kovacevic, and J.A.Kelner, *Quantized Frame Expansions with Erasures*, Applied and Computational Harmonic Analysis 10 (2001), 203–233

[24] V.K.Goyal, M.Vetterli, and N.T.Thao, *Quantized Overcomplete Expansions in RN: Analysis, Synthesis and Algorithms*, IEEE Trans. on Information Theory 44 (1998), 16–31

[25] R. Gribonval, M. Nielsen, *Sparse representations in unions of bases*, IEEE Trans. Inform. Theory 49 (2003), 3320–3325

[26] *Handbook of coding theory. Vol. I, II.* Edited by V. S. Pless, W. C. Huffman and R. A. Brualdi. North-Holland, Amsterdam, 1998.

[27] J. Kovacevic, P. Dragotti, and V. Goyal, *Filter Bank Frame Expansions with Erasures*, IEEE Trans. on Information Theory, 48 (2002), 1439–1450

[28] M. Ledoux, *The concentration of measure phenomenon*, Mathematical Surveys and Monographs, 89. American Mathematical Society, Providence, RI, 2001

[29] M. A. Lifshits, *Gaussian random functions*, Mathematics and its Applications, 322. Kluwer Academic Publishers, Dordrecht, 1995

[30] J. Matousek, *Lectures on discrete geometry*, Graduate Texts in Mathematics, 212. Springer-Verlag, New York, 2002.

[31] S. Mendelson, *Geometric parameters in learning theory*, Geometric aspects of functional analysis, 193–235, Lecture Notes in Mathematics, 1850, Springer, Berlin, 2004

[32] D. Spielman, *The complexity of error-correcting codes*, Fundamentals of Computation Theory, Krakow, Poland, 67–84, Lecture Notes in Computer Science 1279, Springer, Berlin, 1997

[33] D. Spielman, *Constructing Error-Correcting Codes from Expander Graphs*, Emerging applications of number theory (Minneapolis, MN, 1996), 591–600, IMA Vol. Math. Appl., 109, Springer, New York, 1999

[34] J. Tropp, *Recovery of short, complex linear combinations via ℓ_1 minimization*, IEEE Trans. Inform. Theory, to appear

[35] J. Tropp, *Greed is good: Algorithmic results for sparse approximation*, IEEE Trans. Inform. Theory, Vol. 50, Num. 10, October 2004, pp. 2231-2242

[36] J. Tropp, *Just relax: Convex programming methods for subset selection and sparse approximation*, ICES Report 04-04, UT-Austin, February 2004

Departent of Mathematics, University of Missouri, Columbia, MO 65211, U.S.A.
E-mail address: rudelson@math.missouri.edu

Departent of Mathematics, University of California, Davis, CA 95616, U.S.A.
E-mail address: vershynin@math.ucdavis.edu