Least Squares Superposition Codes of Moderate Dictionary Size Are Reliable at Rates up to Capacity

Antony Joseph, *Student Member, IEEE*, and Andrew R Barron, *Senior Member, IEEE*

***Abstract*—For the additive white Gaussian noise channel with average codeword power constraint, coding methods are analyzed in which the codewords are sparse superpositions, that is, linear combinations of subsets of vectors from a given design, with the possible messages indexed by the choice of subset. Decoding is by least squares (maximum likelihood), tailored to the assumed form of codewords being linear combinations of elements of the design. Communication is shown to be reliable with error probability exponentially small for all rates up to the Shannon capacity.**

***Index Terms*—Achieving capacity, compressed sensing, exponential error bounds, Gaussian channel, maximum likelihood estimation, subset selection.**

I. Introduction

THE additive white Gaussian noise channel is basic to Shannon theory and real communication models. In superposition coding schemes, the codewords are sparse linear combinations of elements from a given dictionary. We show that superposition codes from polynomial size dictionaries with maximum likelihood (minimum distance) decoding achieve exponentially small error probability for any communication rate less than the Shannon capacity. A companion paper [8],[9] provides a fast decoding method and its analysis. The developments involve a merging of modern perspectives on statistical linear model selection and information theory.

The familiar communication problem is as follows. Input bit strings $u = (u_1, u_2, \ldots, u_K)$ of length K are mapped into codewords, of length n, with control of their power. The channel adds independent $N(0, \sigma^2)$ noise to the selected codeword yielding a received length n string Y. Using the received string and knowledge of the codebook, the decoder, then, gets an estimate $\hat{u}$ of the transmitted string u. Block error is the event $\hat{u} \neq u$, bit error at position i is the event $\hat{u}_i \neq u_i$, and the bit error rate is $(1/K)\sum_{i=1}^{K} 1_{\{\hat{u}_i \neq u_i\}}$. Analogous section error rate for our code is defined as follows. The reliability requirement is that, with sufficiently large n, the bit error rate or section error rate is small with high probability, when averaged over input strings u as well as the distribution of Y. A more stringent requirement would be to have small block error probability, again averaged over the distributions of u and Y. As will be made clear later on, for ease of analysis, we perform a further averaging over the distribution of our design matrix.

The communication rate $R = K/n$ is the ratio of the input length to the code length for communication across the channel. By traditional information theory, as in [20], [35], and [60], the supremum of reliable rates is the channel capacity $C = (1/2)\log_2(1+P/\sigma^2)$, where P is a constraint on the power of the codewords. Standard communication models, even in continuous time, have been reduced to the aforementioned discrete-time white Gaussian noise setting, as in [31] and [35].

We now describe the superposition coding scheme. The story begins with a dictionary (design matrix) $X \in \mathbb{R}^{n \times N}$, with columns $X_j \in \mathbb{R}^n$ for $j = 1, 2, \ldots, N$. We further assume that $N = LM$, with L and M being positive integers. The dictionary is partitioned into L sections, each of size M as depicted in Fig. 1.

The codewords take the form of particular linear combinations of subsets of columns of the dictionary. Specifically, each codeword is of the form $X\beta$, where $\beta \in \mathbb{R}^N$ belongs to a set $\mathcal{B}$ given by

$$\mathcal{B} = \{\beta \in \{0, 1\}^N : \beta_j \text{ has one 1 in each section}\}$$

Consequently, for $\beta \in \mathcal{B}$, the codeword $X\beta$ is a superposition of L columns of X, with exactly one column selected from each section. The received vector is then in accordance with the statistical linear model

$$Y = X\beta + \epsilon. \tag{1}$$

where ϵ is the noise vector distributed $\text{Normal}(0, \sigma^2 I)$.

For ease of encoding, it is assumed that the section size M is a power of 2. The input bit strings u are of length $K = L\log_2 M$, which split into L substrings of size $\log_2 M$. The encoder maps u to β simply by interpreting each substring of u as giving the index of which coordinate of β is nonzero in the corresponding section. That is, each substring is the binary representation of the corresponding index.

As mentioned earlier, we analyze the maximum likelihood decoder. This decoder is the same as that which chooses the β that maximizes the posterior probability when the prior distribution is uniform over $\mathcal{B}$. The decoder is given by

$$\hat{\beta} = \arg\min_{\beta \in \mathcal{B}} \|Y - X\beta\|^2 \tag{2}$$

where $\|.\|$ denotes the Euclidean norm. Here, we implicitly assume that if the minimization has a nonunique solution, one may take $\hat{\beta}$ to be any value in the solution set. Since the earlier

Manuscript received June 05, 2010; revised July 07, 2011; accepted November 28, 2011. Date of publication January 31, 2012; date of current version April 17, 2012. The material in this paper was presented in part at the 2010 IEEE International Symposium on Information Theory.

The authors are with the Department of Statistics, Yale University, New Haven, CT 06520 USA (e-mail: antony.joseph@yale.edu; andrew.barron@yale.edu).

Communicated by I. Kontoyiannis, Associate Editor for Shannon Theory.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2012.2184847

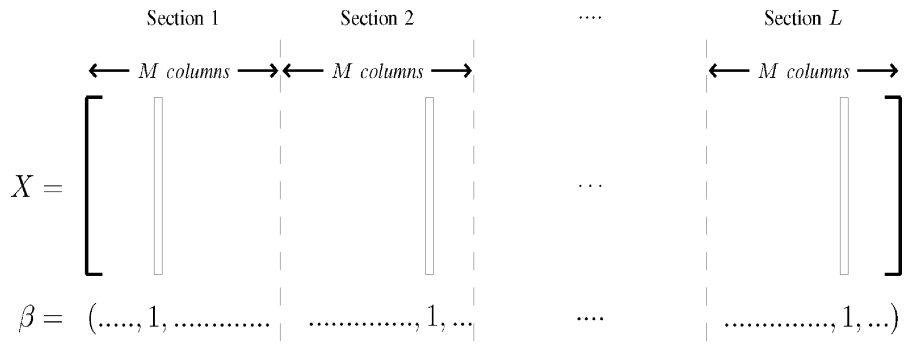

Fig. 1. Schematic rendering of the dictionary matrix X and coefficient vector β. The vertical bars in the X matrix indicate the selected columns from a section.

is a least squares minimization problem over coefficient vectors in $\mathcal{B}$, we also call this the least squares decoder. Although the aforementioned decoder is not a computationally feasible scheme, the result is significant since we show that one can achieve rates up to capacity with a codebook that has a compact representation in the form of the dictionary X.

The entries of X are drawn independently from a normal distribution with mean zero and variance P/L. With this distribution, one has that for each $\beta \in \mathcal{B}$, the expected codeword power, given by $\mathbb{E}\|X\beta\|^2/n$, is equal to P. Our design produces a distribution of codeword powers $\|X\beta\|^2/n$, across the 2^K codewords, that is highly concentrated near P, with average codeword power $(1/2^K)\sum_{\beta\in\mathcal{B}}\|X\beta\|^2/n$ having expectation P. Use of average power rather than individual power constraint does not increase the capacity.

An alternative method would be to arrange the entries of X to be equiprobable $\pm\sqrt{P/L}$ random variables. This would achieve an approximately Gaussian distribution for the $X\beta$'s. It is very likely that this alternative design also achieves capacity, though that is not explored here.

As we have said, the rate of the code is $R = K/n$ input bits per channel uses and we arrange for R arbitrarily close to C. For our code, this rate is $R = (L\log M)/n$. For specified rate R, the code length $n = (L/R)\log M$. As explained in the following, the section size M will be related to the number of sections L by an expression of polynomial size. Consequently, the length n and the number of terms L agree to within a log factor.

Control of the dictionary size is critical to computationally advantageous coding and decoding. If the number of sections L were fixed, then X has size $N = L2^{nR/L}$ that is exponential in n, making its direct use impractical. Instead, with L agreeing with n to within a $\log$ factor, the dictionary size is more manageable. In this setting, we construct reliable, high-rate codes with codewords corresponding to linear combinations of subsets of terms in moderate size dictionaries.

The idea of superposition codes for Gaussian channels began with Cover [19] in the context of determination of the capacity region of certain multiple user channels. There L represents the number of messages decoded and a selected column represents the codeword for a message. Codes for the Gaussian channel based on sparse linear combinations have been proposed in the compressed sensing community by Tropp [64]. However, as he discusses, the rate achieved there is not up to capacity. Relationship of our study to that in these communities will be discussed in further detail later on.

We now describe our main result concerning the performance of the least squares decoder. We show that if $M = L^a$, for any a exceeding a particular positive function of the signal-to-noise ratio v, then rates arbitrarily close to capacity can be achieved. This function is near $16/v^2$ for small v and near 1 for large v. Consequently, the dictionary has size $N = L^{a+1}$ that is polynomial in L. This required section size does not depend on the gap $C - R$, and thus, the dictionary has a compact representation irrespective of the closeness of R to C.

For $\beta \in \mathcal{B}$, let $\mathbb{P}_\beta(.)$ denote the joint distribution of Y, X given β. Further, let $mistakes$ denote the number of mistakes made by the least squares decoder, that is, the number of sections in which the position of the nonzero term in $\hat{\beta}$ is different from that in the true β. Denote the error event

$$\mathcal{E}_{\alpha_0} = \{mistakes \geq \alpha_0 L\} \tag{3}$$

that the decoder makes mistakes in at least α_0 fraction of sections. Assuming that β is drawn from a uniform distribution over all M^L elements from $\mathcal{B}$, the average probability of error conditional on X is given by

$$\bar{\mathbb{P}}\,[\mathcal{E}_{\alpha_0}|X] = \frac{1}{M^L}\sum_{\beta\in\mathcal{B}}\mathbb{P}_\beta[\mathcal{E}_{\alpha_0}|X].$$

Deriving bounds for the aforementioned is not easy. We follow the information theory tradition and bound the average of the earlier over the distribution of X, given by

$$\bar{\mathbb{P}}[\mathcal{E}_{\alpha_0}] = \mathbb{E}_X\bar{\mathbb{P}}[\mathcal{E}_{\alpha_0}|X]. \tag{4}$$

For positive x, let $g(x) = \sqrt{1+4x^2} - 1$. Furthermore, for $R \leq C$, let

$$w_v = \frac{v}{[4(1+v)^2]\sqrt{1+(1/4)v^3/(1+v)}}. \tag{5}$$

A positive expression $a_{v,L}$ possessing properties explained in Section IV, lemma 5 is used. For large L, it is near a function a_v near $16/v^2$ for small v and near 1 for large v. Our main result is the following.

Proposition 1: Assume $M = L^a$, where $a \geq a_{v,L}$, and rate R is less than capacity C. Let α_0 represents the fraction of section mistakes made by the least squares decoder. Then

$$\bar{\mathbb{P}}[\mathcal{E}_{\alpha_0}] = e^{-nE(\alpha_0,R)}$$

with $E(\alpha_0, R) \geq h(\alpha_0, C - R) - (\log 2L)/n$, where

$$h(\alpha, \Delta) = \min\left\{\alpha w_v \Delta,\ \frac{1}{4} g\left(\frac{\Delta}{2\sqrt{v}}\right)\right\} \tag{6}$$

is evaluated at $\alpha = \alpha_0$ and $\Delta = C - R$.

Proposition 1 is proved in Section V.

Remark: It is shown in Appendix C that the exponent $E(\alpha_0, R)$ can be improved by replacing $h(\alpha_0, C - R)$ with $\tilde{h}(\alpha_0, C - R)$ where

$$\tilde{h}(\alpha, \Delta) = \min\left\{c_{\alpha,v}\,\alpha,\ \frac{1}{4} g\left(\frac{\Delta}{2\sqrt{v}}\right)\right\}.$$

Here, $c_{\alpha,v}$ is a positive function of α and v, which for given v is near $\tau_v \tilde{w}_v/4$ for small α, where τ_v and $\tilde{w}_v$ are positive expressions as in (43) and (44) shown later.

Let $g^*(x) = \min\{\sqrt{2}x,\ x^2\}$. Then, it is not hard to see that

$$g(x) \geq g^*(x) \quad \text{for all} \quad x \geq 0. \tag{7}$$

Accordingly, the function $g(.)$, appearing in the lower bound (6), may be replaced by $g^*(.)$, revealing that the exponent is, up to a constant, of the form $\min\{\alpha_0\Delta,\ \Delta^2\}$, where $\Delta = C - R$. With the improved bound in Appendix C, it is of the form $\min\{\alpha_0,\ \Delta^2\}$.

Moreover, an approach is discussed which completes the task of identifying the terms by arranging sufficient distance between the subsets, using composition with an outer Reed–Solomon (RS) code of rate near one. It corrects the small fraction of remaining mistakes so that we end up not only with small mistake rate but also with small block error probability. If $R_{\text{outer}} = 1 - \delta$ is the rate of an RS code, with $0 < \delta < 1$, then section error rates less than α_0 can be corrected, provided $2\alpha_0 < \delta$. Furthermore, if R_{inner} (or simply R) is the rate associated with our inner (superposition) code, then the total rate after correcting for the remaining mistakes is given by $R_{\text{total}} = R_{\text{inner}} R_{\text{outer}}$. The end result, using our theory for the distribution of the fraction of mistakes of the superposition code, is that the block error probability is exponentially small. One may regard the composite code as a superposition code in which the subsets are forced to maintain at least a certain minimal separation, so that decoding to within a certain distance from the true subset implies exact decoding. Accordingly, we make the following claim about block error probability.

Proposition 2: For given fraction of mistakes α_0, let R be a rate for which the partitioned superposition code with L sections has exponentially small probability $\epsilon_n = \bar{\mathbb{P}}\{\mathcal{E}_{\alpha_0}\}$ of Proposition 1. Then, through concatenation with an outer RS code, one obtains a code with rate $(1 - 2\alpha_0)R$ and block error probability less than or equal to ϵ_n.

Proposition 2 is proved in Section VI.

Particular interest is given to the case that the rate R is made to approach the capacity C. Arrange $R = C - \Delta_n$ and $\alpha_0 = \Delta_n$. One may let the rate gap Δ_n tend to zero (e.g., at a $1/\log n$ rate or any polynomial rate not faster than $1/\sqrt{n}$); then, the overall rate $R_{\text{tot}} = (1 - 2\alpha_0)(C - \Delta_n)$ continues to have drop from capacity of order Δ_n, with the composite code having block error probability of order

$$\exp\{-nc\Delta_n^2\}.$$

The aforementioned exponent, of order $(C–R)^2$ for R near C, is in agreement with the form of the optimal reliability bounds as in [35] and [53], though, here, our constant c is not demonstrated to be optimal.

In Fig. 2, we plot curves of achievable rates using our scheme for block error probability fixed at 10^{-4} and signal-to-noise ratios of 20 and 100. We also compare this to a rate curve given in [53] (PPV curve), where it is demonstrated that for a Gaussian channel with signal-to-noise ratio v, the block error probability ϵ, code length n, and rate R with an optimal code can be well approximated by the following relation:

$$R \approx C - \sqrt{\frac{V}{n}} Q^{-1}(\epsilon) + \frac{1}{2}\frac{\log n}{n} \tag{8}$$

where $V = (v/2)(v + 2)\log^2 e/(v + 1)^2$ is the channel dispersion and Q^{-1} is the inverse normal cumulative distribution function.

For the superposition code curve, the y-axis gives the highest R_{comp} for which the error probability stays below 10^{-4}. We see for the given v and block error probability values, the achievable rates using our scheme are reasonably close to the theoretically best scheme. Note that the PPV curve was computed with an approach that uses a codebook of size that is exponential in block length, whereas our dictionary, of size LM, is of considerably smaller size.

A. Variants of the Superposition Scheme

To distinguish it from other sparse superposition codes, the code analyzed here may be called a *partitioned superposition* code. The motivations for introducing the partitioning versus arbitrary subsets, in the superposition coding scheme, are the ease in mapping the input bit string to the coefficient vector and the ease in composition with the outer RS code. Natural variants of the schemes are *subset superposition* coding, where one arranges for a number L of the coordinates to be nonzero and taking the value 1, with the message conveyed by the choice of subset. With somewhat greater freedom, one may have *signed superposition* coding, where one arranges the nonzero coefficients to be $+1$ or -1. Then, the message is conveyed by the sequence of signs as well as the choice of subset. In both cases, if one takes the elements of X to be i.i.d $N(0, P/L)$ as before, then the expected power of each codeword is P. The signed superposition coding scheme has been proposed in [36] and [64].

As mentioned earlier, superposition codes began with [19] for multiuser channels in the context of determination of the capacity region of Gaussian broadcast channels. There the number of users corresponds to L. The codewords for user ℓ, for $\ell = 1, \ldots, L$, corresponds to the columns in section ℓ. In that setting, what is sent is the sum of codewords, one from each user. With L fixed, $M = 2^{nR/L}$ is exponential in L. Here, for the

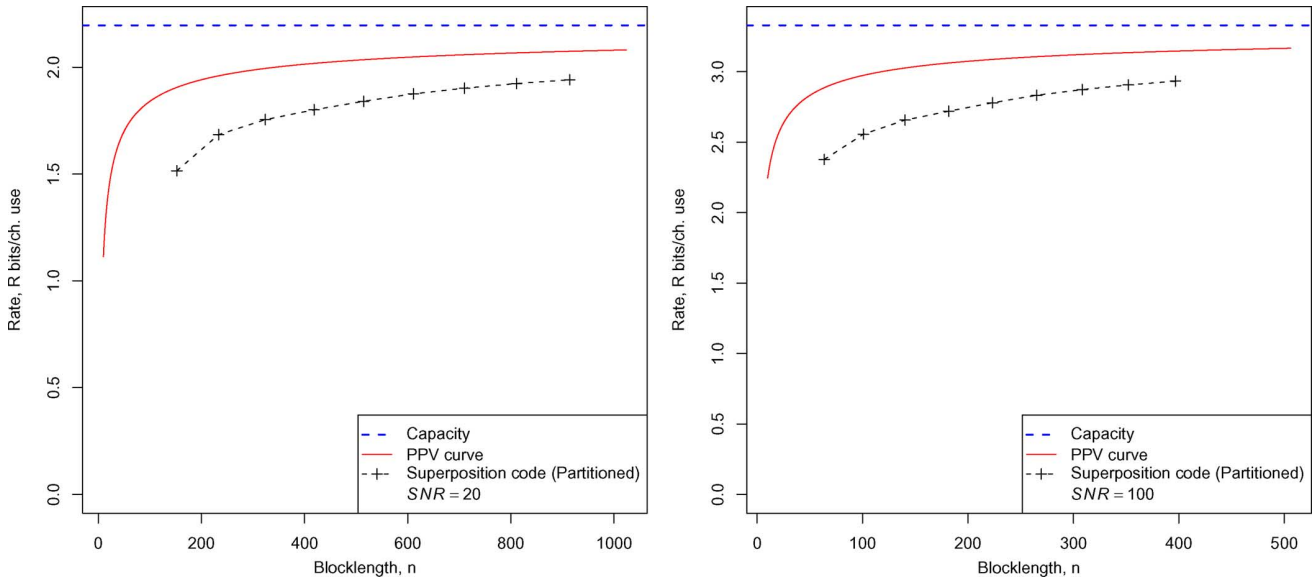

Fig. 2. Plot of comparison between achievable rates using our scheme and the theoretical best possible rates for *block error* probability of 10^{-4} and signal-to-noise ratio (v) values of 20 and 100. The curves for our partitioned superposition code were evaluated at points with number of sections L ranging from 20 to 100 in steps of 10, with corresponding M values taken to be L^{a_v}, where a_v is as given in Lemma 5, (32), and (33) later on. For the v values of 20 and 100 shown previously, a_v is around 2.6 and 1.6, respectively. For details on computations, refer to Appendix D.

single-user channel, by allowing L to be of the same order as n, to within a log factor, we make it possible to achieve rates close to capacity with polynomial size dictionaries. Related rate splitting (partitioning) for superposition codes is developed for Gaussian multiple-access problems in [18] and [59].

As to the relationship to single-user decoding, note that in the Gaussian broadcast channel, with optimal decoding, it is arranged that one of the receivers decodes all the messages. This is also the case for the multiple access channel receiver. The terminology of superposition codes, rate splitting (partitioning), and issues of power allocations arise from such work in multiuser Shannon theory. Here, to achieve the benefits of the reduced size dictionary, we decode the sections jointly rather than successively. Here, it does allow the power allocation to be constant across sections. In the companion paper [8], in achieving a practical decoder, we do make use of standard variable power allocation in the sections.

Sparse superposition codes have been proposed for communication in random access channels as in [14] and [27].

Our ideas of sparse superposition coding are adapted to Gaussian vector quantization in [42].

B. Related Work on Sparse Signal Recovery

While reviewing works on sparse signal recovery and compressed sensing, we adhere to our notation that we have a linear model of the form

$$Y = X\beta + \epsilon$$

where $X \in \mathbb{R}^{n\times N}$ is a deterministic or random matrix and $\beta \in \mathbb{R}^N$ has exactly L nonzero values. The quantities n, N, L, and β will be called parameters for the model. In our description in the following, we denote as *const* some positive constant whose value will change from time to time.

The conclusions here complement recent work on sparse signal recovery in the linear model setup as we now discuss. In a broad sense, these works analyze for various schemes (practical or otherwise), conditions on the parameters so that certain reliability requirements are satisfied with high probability. Closely related to our work is the requirement that only the indices corresponding to the nonzero elements of β, that is the support of β, be recovered exactly or almost exactly. The conditions explored by this community do translate into results on communication rate, though heretofore not rates up to capacity.

In this paper, in order to achieve rates arbitrarily close capacity, we require $N = L^{a+1}$, with precise values of a specified later on, putting us in the sublinear sparsity regime, that is, $L/N \to 0$ as $L, N \to \infty$. Also, if we change the scale and take the elements of the X matrix as i.i.d standard normal, the nonzero values of β assume the value $\sqrt{P/L}$. Accordingly, although most the claims in this area are for more general sparsity regimes and values of β, the results most relevant to us are those for the sublinear sparsity regime and when the nonzero β_j's are at least $const/\sqrt{L}$.

A significant portion of the work in this area focuses on deterministic X matrices satisfying certain assumptions. A common assumption is the mutual incoherence condition [15], [24], [33] which places controls on the magnitude correlation between distinct pairs of columns. Another related assumption is the exact recovery condition [64], [68], [72]. The recovery uses ℓ_1-relaxation methods such as Lasso [62] or iterative methods such as orthogonal matching pursuit [49], [52]. This line has been pursued by the authors in [23], [24], [32], [70], [72], and others, for general sparse signal recovery problems and by Tropp [64] for the communication problem. While the aforementioned covers broad classes of dictionaries, they impose severe constraints on the dictionaries. Indeed, when applied to Gaussian X matrices, they require $n \geq const\, L^2 \log N$ or sparsity $L \leq const\sqrt{n/\log N}$, which would correspond to rate approaching 0. In contrast, for our scheme $n = (L/R)\log M$, which using $L = M^a$

and $N = LM$, one gets that $n = [a/R(a+1)]\, L \log N$ is sufficient for subset recovery, which is of a smaller order of magnitude than the aforementioned. Consequently, these results on deterministic X matrices, when applied to our setting, are insufficient to communicate at positive rates, let alone rates close to capacity.

The aforementioned works allow for decoding of arbitrary sparse subsets with high probability. This rather stringent form of conclusion corresponds to worst case error probability in the communication setting.

Work which does correspond to positive rate, when translated to the communication setting, arises from three approaches. First, there is the work of Candes and Plan [15] and Tropp [65], [66], in which one looks at the probability of error averaged over codewords (i.e., the subset is chosen randomly). This achieves reliable support recovery with L as high as $const\, n/\log N$. Second, there is the work of Zhang [71] that employs a more involved forward/backward stepwise selection algorithm, for dictionaries satisfying certain properties, to achieve reliable performance for arbitrary subsets (worst case error probability), again for L as high $const\, n/\log N$. However, the constants are such that demonstration that rates up to capacity can be achieved has been lacking.

Third, analysis using random X matrices in the noisy setting has also been carried out in [17], [22], and [68], among others, where the analysis in [68] addresses the issue of support recovery. More closely related to ours, support recovery of the least squares decoder is analyzed in [2], [28], and [67], for Gaussian X matrices, where Akcakaya and Tarokh [2] also address the issue of partial support recovery. Similar to aforementioned, one can infer from this that communication at positive rates is possible using random designs. The signal recovery purpose is somewhat different here from our communications purpose, in that the work typically does not constrain the nonzero coefficients to the same value, and the resulting freedom in their values lead to order of magnitude conclusions that obstruct interpretation in terms of exact rate.

Furthermore, there are result giving necessary conditions for exact support recovery [29], [67], [69] and for partial support recovery [2]. Both these agree in terms of order of magnitude, requiring an order of $L \log N$ for the regime we deal with. In [56], it is shown that in the linear sparsity regime, that is, when L is of the same order as N, one requires $n \geq const N$ for reliable recovery of the support. An implication of this is that the sublinear sparsity regime is necessary for communication at positive rates.

Consequently, one can infer, from some of the aforementioned works, that communication at positive rates is possible with sparse superposition codes. We add to the existing literature by showing that one can achieve any rate up to capacity in certain sparsity regimes with a compact dictionary, albeit for a computationally infeasible scheme. Furthermore, we demonstrate that the error exponents are of the optimal form.

C. Practical Decoding Algorithms Approaching Capacity

Along with this paper, we pursued the problem of achieving capacity using computationally feasible schemes. In [8] and [9], an iterative decoding scheme, called adaptive successive decoding, is analyzed. This is similar in spirit to iterative decoding techniques such as forward stepwise regression [7], [41], relaxed greedy algorithm [6], [38], [44], and orthogonal matching pursuit [49], [52], and other iterative algorithms [13], [21], [51]. The rate attained there is of the order of $1/\log M$ below capacity, with corresponding error probability being exponentially small in $L/(\log M)^2$. These performance levels are not as good as obtained here with the optimal decoder. The sparse superposition codes achieving these performance levels, by least squares and by adaptive successive decoding, are different in an important aspect. For this paper, we use a constant power allocation, with the same power P/L for each term. However, in [8] and [9], to yield rates near capacity, we needed a variable power allocation, achieved by a specific schedule of the nonzero β_j's. In contrast, if one were to use equal power allocation for the decoding scheme, then reliable decoding holds only up to a threshold rate $R_{\text{thres}} = (1/2)P/(P+\sigma^2)$, which is less than the capacity C. Since the focus here is on the least squares decoder, we defer detailed discussion to the later paper [9].

D. Related Communication Issues and Schemes

The development, here, is specific to the discrete-time channel for which $Y_i = c_i + \varepsilon_i$ for $i = 1, 2, \ldots, n$ with real-valued inputs and outputs and with independent Gaussian noise.

Standard approaches, as discussed in [31], entail a decomposition of the problem into separate problems of coding and of shaping of a multivariate signal constellation. Notice that we build shaping directly into the coding scheme by choosing codewords to follow a $\text{Normal}(0, P)$ distribution.

For the low signal-to-noise regime, binary codes suffice for communication near capacity and there is no need for shaping. The performance of the maximum likelihood decoder for binary linear codes, with a random design matrix and with exponential error bounds at rates up to capacity for the binary symmetric channel, has been established in [26]. Computationally feasible schemes, with empirically good performance, for discrete channels include LDPC codes [34], [46], [47], [57], [58] and turbo codes [12], [50]. Error bounds for rates up to capacity for expander codes (related to LDPC) are shown in [5] and for LDPC codes with random low-density design matrix in [43], whereas turbo codes have an error floor [37], [54] that precludes such exponential scaling of error probability. Thus, the work in [5], [26], and [43], with a random design matrix of controlled size, are conclusions for discrete channels that correspond to the conclusion obtained here for the Gaussian channel for rates up to capacity.

Recently, practical and capacity-achieving polar codes have been developed for discrete channels [3], [4], though with an error probability that is exponentially small in $\sqrt{n}$ rather than n. Unlike the present development, it remains unknown how the exponent for the polar codes depends on the closeness of R to C.

When the signal-to-noise ratio is not small, proper shaping for the Gaussian channel requires larger size signal alphabets, as explained in [31]. For example, Abbe and Barron [1] provide such analysis adapting polar codes to use for the Gaussian channel.

The analysis of concatenated codes in [30] is an important forerunner to the development we give here. The author in [30] identified benefits of an outer RS code paired in theory with an optimal inner code of Shannon–Gallager type and in practice with binary inner codes based on linear combinations of orthogonal terms (for target rates K/n less than 1 such a basis is available). The challenge concerning theoretically good inner codes is that the number of messages searched is exponentially large in the inner code length. Forney made the inner code length of logarithmic size compared to the outer code length as a step toward practical solution. However, caution is required with such a strategy. Suppose the rate of the inner code has only a small drop from capacity, $\Delta = C - R$. For small inner code error probability, the inner code length must be of order at least $1/\Delta^2$. So with that scheme, one has the undesirable consequence that the required outer code length becomes exponential in $1/\Delta^2$.

For the Gaussian noise channel, our tactic to overcome that difficulty uses a superposition inner code with a polynomial size dictionary. We use inner and outer code lengths that are comparable, with the outer code used to correct errors in a small fraction of the sections of the inner code. The overall code length to achieve error probability ϵ remains of the order $(1/\Delta^2)\log(1/\epsilon)$.

Section II contains brief preliminaries. Section III provides core lemmas on the reliability of least squares for our superposition codes. Section IV analyzes the matter of section size sufficient for reliability. In Sections V and VI, we give proofs of propositions 1 and 2, respectively. In Section VII, we discuss how our results can be adapted for an approximate form of the least squares decoder. The Appendix collects some auxiliary matters.

II. Preliminaries

For vectors $a \text{and} b$ of length n, let $||a||^2$ be the sum of squares of coordinates, let $|a|^2 = (1/n)\sum_{i=1}^n a_i^2$ be the average square, and let $a \cdot b = (1/n)\sum_{i=1}^n a_i b_i$ be the associated inner product. It is a matter of taste, but we find it slightly more convenient to work, henceforth, with the norm $|a|$ rather than $||a||$.

Concerning the base of the logarithm (log) and associated exponential (exp), base 2 is most suitable for interpretation and base e most suitable for the calculus. For instance, the rate $R = (L \log M)/n$ is measured in bits if the log is base 2 and nats if the log is base e. Typically, conclusions are stated in a manner that can be interpreted to be invariant to the choice of base, and base e is used for convenience in the derivations.

We make repeated use of the following moment generating function and its associated Cramer–Chernoff large deviation exponent in constructing bounds on error probabilities. If Z and $\tilde{Z}$ are normal with means equal to 0, variances equal to 1, and correlation coefficient ρ, then

$$\mathbb{E}(e^{(\lambda/2)(Z^2-\tilde{Z}^2)}) = 1/[1-\lambda^2(1-\rho^2)]^{1/2} \tag{9}$$

when $\lambda^2 < 1/(1-\rho^2)$ and infinity otherwise. So, taking the logarithm, the associated cumulant generating function of $(1/2)(Z^2 - \tilde{Z}^2)$ is $-(1/2)\log(1-\lambda^2(1-\rho^2))$, with the understanding that the minus log is replaced by infinity when λ^2 is at least $1/(1-\rho^2)$. For positive Δ, we define the quantity $D = D(\Delta, 1-\rho^2)$ given by

$$D = \max_{\lambda \geq 0} \{\lambda\Delta + (1/2)\log(1-\lambda^2(1-\rho^2))\}. \tag{10}$$

The expression corresponding to D but with the maximum restricted to $0 \leq \lambda \leq 1$ is denoted as $D_1 = D_1(\Delta, 1-\rho^2)$, that is

$$D_1 = \max_{0 \leq \lambda \leq 1} \{\lambda\Delta + (1/2)\log(1-\lambda^2(1-\rho^2))\}. \tag{11}$$

When the optimal λ is strictly less than 1, the value of D_1 matches D as given previously.

The $\lambda = 1$ case occurs when $1 + 4\Delta^2/(1-\rho^2) \geq (1+2\Delta)^2$, or equivalently $\Delta \geq (1-\rho^2)/\rho^2$. Then, the exponent is $D_1 = \Delta + (1/2)\log\rho^2$, which is as least $\Delta - (1/2)\log(1+\Delta)$. Consequently, in this regime, D_1 is between $\Delta/2$ and Δ. The special case $\rho^2 = 1$ is included with $D_1 = \Delta$.

There is a role for the function

$$C_\alpha = \frac{1}{2}\log(1+\alpha v) \tag{12}$$

for $0 \leq \alpha \leq 1$, where $v = P/\sigma^2$ is the signal-to-noise ratio and $C_1 = C = (1/2)\log(1+v)$ is the channel capacity. We note that $C_\alpha - \alpha C$ is a nonnegative concave function equal to 0 when α is 0 or 1 and strictly positive in between. The quantity $C_\alpha - \alpha R$ is larger by the additional amount $\alpha(C-R)$, positive when the rate R is less than the Shannon capacity C.

Remark on average codeword power: The average codeword power $M^{-L}\sum_{\beta \in \mathcal{B}} |X\beta|^2$ has expectation with respect to X that matches $\mathbb{E}|X\beta|^2 = P$, for all $\beta \in \mathcal{B}$. The distribution of the average codeword power is tightly concentrated around P as explained in the [11, Appendix], and will not be explored further here.

III. Performance of Least Squares

In this section, we examine the performance of the least squares decoder (2) in terms of rate and reliability. For $\beta \in \mathcal{B}$, let $S(\beta) = \{j : \beta_j = 1\}$ denote the set of indices for which β is nonzero. Furthermore, let

$$\mathcal{A} = \{S(\beta) : \beta \in \mathcal{B}\} \tag{13}$$

denote the set of allowed subset of terms. It corresponds to the M^L subsets of $\{1, \ldots, N\}$ of size L and comprising of exactly one term from each section.

Recall that we are interested in bounding $\bar{\mathbb{P}}[\mathcal{E}_{\alpha_0}]$ given in (4). By symmetry

$$\bar{\mathbb{P}}[\mathcal{E}_{\alpha_0}] = \mathbb{P}_\beta[\mathcal{E}_{\alpha_0}] \quad \text{for all} \quad \beta \in \mathcal{B}$$

where $\mathbb{P}_\beta[\mathcal{E}_{\alpha_0}] = \mathbb{E}_X \mathbb{P}_\beta[\mathcal{E}_{\alpha_0}|X]$. Correspondingly, for fixed $\beta^* \in \mathcal{B}$, we proceed to obtain bounds for $\mathbb{P}_{\beta^*}[\mathcal{E}_{\alpha_0}]$. Let $S^* = S(\beta^*)$. Furthermore, let $\hat{\beta}$ be the least squares solution (2) and $\hat{S} = S(\hat{\beta})$. Notice that $mistakes = card(\hat{S} - S^*)$, which is also the number of sections incorrectly decoded.

For $\ell \in \{1, 2\ldots, L\}$, let $E_\ell = \{mistakes = \ell\}$ be the event that there are exactly ℓ mistakes. Now, $\mathcal{E}_{\alpha_0}$ can be expressed as a disjoint union of E_ℓ, for $\ell \geq \alpha_0 L$. Correspondingly

$$\mathbb{P}_{\beta^*}[\mathcal{E}_{\alpha_0}] = \sum_{\ell \geq \alpha_0 L} \mathbb{P}_{\beta^*}[E_\ell]. \tag{14}$$

In the following two lemmas, we give bounds for $\mathbb{P}_{\beta^*}(E_\ell)$ for $\ell = 1, \ldots, L$.

Lemma 3: Set $\alpha = \ell/L$ for an $\ell \in \{1, 2, \ldots, L\}$. The probability $\mathbb{P}_{\beta^*}(E_\ell)$ can be bounded by $err_1(\alpha)$, where

$$err_1(\alpha) = \binom{L}{\alpha L} \exp\left\{-nD_1(\Delta_\alpha, 1-\rho_\alpha^2)\right\} \tag{15}$$

where $\Delta_\alpha = C_\alpha - \alpha R$ and $1 - \rho_\alpha^2 = \alpha v/(1+\alpha v)$. Here, v is the signal-to-noise ratio.

Remark: Notice that $err_1(\alpha)$ depends also on L, n, and v. Whether $err_1(\alpha)$ is exponentially small depends on the relative size of the combinatorial term $\binom{L}{\alpha L}$ and the exponential term in n and α.

Proof of Lemma 3: For the occurrence of E_ℓ, there must be an $S \in \mathcal{A}$ which differs from the subset S^* sent in an amount $card(S - S^*) = card(S^* - S) = \ell$ and which has $|Y - X_S|^2 \leq |Y - X_{S^*}|^2$, or equivalently has $T(S) \leq 0$, where

$$T(S) = \frac{1}{2}\left[\frac{|Y - X_S|^2}{\sigma^2} - \frac{|Y - X_{S^*}|^2}{\sigma^2}\right]. \tag{16}$$

The analysis proceeds by considering an arbitrary such S, bounding the probability that $T(S) \leq 0$, and then using an appropriately designed union bound to put such probabilities together. Notice that the subsets S and S^* have an intersection $S_1 = S \cap S^*$ of size $L - \ell$ and difference $S_2 = S - S_1$ of size $\ell = \alpha L$.

Let $p(Y, X)$ denote the joint density of Y and X when S^* is sent. Furthermore, let $X_{S_1} = \sum_{j \in S_1} X_j$. The actual density of Y given X_{S_1}, denoted by $p(Y|X_{S_1})$, has mean X_{S_1} and variance $(\sigma^2 + \alpha P)I$. Furthermore, there is conditional independence of Y and X_{S_2} given X_{S_1}.

Next, consider the alternative hypothesis that S was sent and let $p_h(Y, X)$ denote the corresponding joint density under this hypothesis. The conditional density for Y given X_{S_1} and X_{S_2}, denoted by $p_h(Y|X_{S_1}, X_{S_2})$, is now Normal$(X_S, \sigma^2 I)$. With respect to this alternative hypothesis, the conditional distribution for Y given X_{S_1} remains Normal$(X_{S_1}, (\sigma^2 + \alpha P)I)$. That is, $p_h(Y|X_{S_1}) = p(Y|X_{S_1})$.

We decompose the test statistic $T(S)$ in (16) as $T_1 + T_2$, where

$$T_1 = \frac{1}{2}\left[\frac{|Y - X_{S_1}|^2}{\sigma^2 + \alpha P} - \frac{|Y - X_{S^*}|^2}{\sigma^2}\right] \tag{17}$$

and

$$T_2 = \frac{1}{2}\left[\frac{|Y - X_S|^2}{\sigma^2} - \frac{|Y - X_{S_1}|^2}{\sigma^2 + \alpha P}\right]. \tag{18}$$

Note that $T_1 = T_1(S_1)$ depends only on terms in S^*, whereas $T_2 = T_2(S)$ depends also on the part of S not in S^*.

Concerning T_2, note that we may express it as

$$T_2(S) = \frac{1}{n}\log\frac{p(Y|X_{S_1})}{p_h(Y|X_S)} + C_\alpha \tag{19}$$

where

$$C_\alpha = \frac{1}{2}\log\left(1 + \alpha\frac{P}{\sigma^2}\right)$$

is the adjustment by the logarithm of the ratio of the normalizing constants of these densities. Using Bayes rule, notice that

$$\frac{p_h(X_{S_2}|Y, X_{S_1})}{p(X_{S_2})} = \frac{p_h(Y|X_{S_1}, X_{S_2})}{p(Y|X_{S_1})}.$$

Correspondingly, one gets from (19) that

$$T_2(S) = \frac{1}{n}\log\frac{p(X_{S_2})}{p_h(X_{S_2}|Y, X_{S_1})} + C_\alpha. \tag{20}$$

We are examining the event E_ℓ that there is an $S \in \mathcal{A}$, with $card(S - S^*) = \ell$ and $T(S) \leq 0$. For positive λ, the indicator of this event satisfies

$$1_{E_\ell} \leq \sum_{S_1}\left(\sum_{S_2} e^{-nT(S)}\right)^\lambda$$

where $S_1 = S \cap S^*$ is of size $L - \ell$ and $S_2 = S - S_1$ of size ℓ. The earlier follows since if there is such an S with $T(S) \leq 0$, then indeed that contributes a term on the right side of value at least 1. Here, the outer sum is over $S_1 \subset S^*$. For each such S_1, for the inner sum, we have ℓ sections in each of which, to comprise S_2, there is a term selected from among $B - 1$ choices other than the one prescribed by S^*.

To bound the probability of E_ℓ, take the expectation of both sides, bring the expectation on the right inside the outer sum, and write it as the iterated expectation, where on the inside condition on Y, X_{S_1}, and X_{S^*} to pull out the factor involving T_1, to get that $\mathbb{P}_{\beta^*}[E_\ell]$ is not more than

$$\sum_{S_1} \mathbb{E}e^{-n\lambda T_1(S_1)} \mathbb{E}_{X_{S_2}|Y, X_{S_1}, X_{S^*}}\left(\sum_{S_2} e^{-nT_2(S)}\right)^\lambda.$$

Notice that $p(X_{S_2}|Y, X_{S_1}, X_{S^*}) = p(X_{S_2})$, that is, X_{S_2} is independent of Y, X_{S_1}, and X_{S^*}. Correspondingly, the inner expectation may be expressed as $\mathbb{E}_{X_{S_2}}(.)$. Furthermore, we arrange for λ to be not more than 1. Then, by Jensen's inequality, the expectation $\mathbb{E}_{X_{S_2}}(.)$ may be brought inside the λ power and inside the inner sum, yielding

$$\mathbb{P}_{\beta^*}[E_\ell] \leq \sum_{S_1} \mathbb{E}e^{-n\lambda T_1(S_1)}\left(\sum_{S_2} \mathbb{E}_{X_{S_2}} e^{-nT_2(S)}\right)^\lambda. \tag{21}$$

Recall that

$$e^{-nT_2(S)} = \frac{p_h(X_{S_2}|Y, X_{S_1})}{p(X_{S_2})} e^{-nC_\alpha}$$

from (20). Consequently, one has

$$\mathbb{E}_{X_{S_2}} e^{-nT_2(S)} = \mathbb{E}_{X_{S_2}|Y, X_{S_1}} e^{-nC_\alpha}$$

which is equal to e^{-nC_α}. The sum over S_2 entails less than $B^\ell = e^{nR\alpha}$, where $\alpha = \ell/L$, choices so the bound (21) becomes

$$\mathbb{P}_{\beta^*}[E_\ell] \le \sum_{S_1} \mathbb{E} e^{-n\lambda T_1(S_1)} e^{-n\lambda[C_\alpha - \alpha R]}. \qquad (22)$$

The sum over S_1 in the aforementioned expression is over $\binom{L}{\alpha L}$ terms. Furthermore, $nT_1(S_1)$ is a sum of n independent mean-zero random variables each of which is the difference of squares of normals for which the squared correlation is $\rho_\alpha^2 = 1/(1+\alpha v)$. So using (9), the expectation $\mathbb{E}e^{-n\lambda T_1(S_1)}$ is found to be equal to $[1/[1-\lambda^2\alpha v/(1+\alpha v)]]^{n/2}$. When plugged in earlier and optimized over λ in $[0,1]$, one gets from the expression of D_1 given in (11) that the expectation in the right side of (22) is equal to $e^{-nD_1(\Delta_\alpha, 1-\rho_\alpha^2)}$. This completes the proof of the lemma.

Remark: A natural question to ask is why we did not use the simpler union bound for $\mathbb{P}_{\beta^*}(E_\ell)$ given by

$$\binom{L}{\ell} M^\ell \, \mathbb{P}_{\beta^*}[T(S) \le 0]$$

where $S \in \mathcal{A}$, is any set with $card(S - S^*) = \ell$. One could then use a Chernoff bound for the term $\mathbb{P}_{\beta^*}[T(S) \le 0]$. Indeed, this is what we tried initially; however, due to the presence of the two combinatorial terms, we were unable to make the aforementioned go to zero, with large n, for all rates less than capacity. In our aforementioned proof, by introducing the λ term in the exponent, we were able to reduce the B^ℓ term to $B^{\lambda\ell}$. Optimizing over λ revealed the best bound using this method. Somewhat similar analysis has been done before to obtain error exponent for the standard channel coding problem, for example, in [35].

A difficulty with the Lemma 3 bound is that for α near 1 and for R correspondingly close to C, in the key quantity $\Delta_\alpha^2/(1-\rho_\alpha^2)$, the order of Δ_α^2 is $(1-\alpha)^2$, which is too close to zero to cancel the effect of the combinatorial coefficient $\binom{L}{\alpha L}$.

The following lemma refines the analysis of Lemma 3, obtaining the same exponent with an improved correlation coefficient. The denominator of $\Delta_\alpha^2/(1-\rho_\alpha^2)$ now becomes $\alpha(1-\alpha)/(1+\alpha v)$. This is an improvement due to the presence of the factor $(1-\alpha)$ allowing the conclusion to be useful also for α near 1. The price we pay is the presence of an additional term in the bound.

Lemma 4: Let a positive integer $\ell \le L$ be given and let $\alpha = \ell/L$. Then, $\mathbb{P}_{\beta^*}[E_\ell]$ is bounded by the minimum for t_α in the interval $[0, C_\alpha - \alpha R]$ of $err_2(\alpha, t_\alpha)$, where

$$err_2(\alpha, t_\alpha) = \binom{L}{L\alpha} \exp\left\{-nD_1(\triangle_\alpha, 1-\rho_\alpha^2)\right\} + \exp\left\{-nD(t_\alpha, \alpha^2 v/(1+\alpha^2 v))\right\} \qquad (23)$$

where, here, the quantities $\triangle_\alpha = C_\alpha - \alpha R - t_\alpha$ and $1-\rho_\alpha^2 = \alpha(1-\alpha)v/(1+\alpha v)$.

Proof of Lemma 4: Split the test statistic $T(S) = \tilde{T}(S) + T^*$ where

$$\tilde{T}(S) = \frac{1}{2}\left[\frac{|Y - X_S|^2}{\sigma^2} - \frac{|Y - (1-\alpha)X_{S^*}|^2}{\sigma^2 + \alpha^2 P}\right]$$

and

$$T^* = \frac{1}{2}\left[\frac{|Y - (1-\alpha)X_{S^*}|^2}{\sigma^2 + \alpha^2 P} - \frac{|Y - X_{S^*}|^2}{\sigma^2}\right].$$

Take positive $\tilde{t} = t_\alpha$ and negative $t^* = -t_\alpha$. Then, $E_\ell \subseteq \tilde{E}_\ell \cup E_\ell^*$, with $\tilde{E}_\ell$ being the event that there is an $S \in \mathcal{A}$, with $card(S - S^*) = \ell$ and $\tilde{T}(S) \le \tilde{t}$. Similarly, E_ℓ^* is the corresponding event that $T^* \le t^*$. The part T^* has no dependence on S so its treatment is more simple. It is a mean zero average of differences of squared normal random variables, with squared correlation $1/(1+\alpha^2 v)$. So using its moment generating function, $\mathbb{P}_{\beta^*}[E_\ell^*]$ is exponentially small, bounded by the second of the two expressions in (23).

Concerning $\mathbb{P}_{\beta^*}[\tilde{E}_\ell]$, its analysis is much the same as for Lemma 3. We again decompose $\tilde{T}(S)$ as the sum $\tilde{T}_1(S_1) + \tilde{T}_2(S)$, where $\tilde{T}_2(S) = T_2(S)$ is the same as earlier. The difference is that in forming $\tilde{T}_1(S_1)$ we subtract $\frac{|Y-(1-\alpha)X_{S^*}|^2}{\sigma^2+\alpha^2 P}$ rather than $\frac{|Y-X_{S^*}|^2}{\sigma^2}$. Consequently

$$\tilde{T}_1(S_1) = \frac{1}{2}\left[\frac{|Y - X_{S_1}|^2}{\sigma^2 + \alpha P} - \frac{|Y - (1-\alpha)X_{S^*}|^2}{\sigma^2 + \alpha^2 P}\right]$$

which again involves a difference of squares of standardized normals. But here the coefficient $(1-\alpha)$ multiplying X_{S^*} is such that we have maximized the correlations between the $Y - X_{S_1}$ and $Y - (1-\alpha)X_{S^*}$. Consequently, we have reduced the spread of the distribution of the differences of squares of their standardizations as quantified by the cumulant generating function. One finds that the squared correlation coefficient is $\rho_\alpha^2 = (1+\alpha^2 v)/(1+\alpha v)$ for which $1-\rho_\alpha^2 = \alpha(1-\alpha)v/(1+\alpha v)$. Accordingly we have that the moment generating function is $Ee^{-n\lambda\tilde{T}(S_1)} = \exp\{-(n/2)\log[1-\lambda^2(1-\rho_\alpha^2)]\}$ which gives rise to the bound appearing as the first of the two expressions in (23). This completes the proof of Lemma 4.

From Lemma 4, one gets that $\mathbb{P}_{\beta^*}[E_\ell] \le err_2(\alpha)$, where

$$err_2(\alpha) = \min_{t_\alpha \in [0, C_\alpha - \alpha R]} err_2(\alpha, t_\alpha).$$

Consequently, from Lemmas 3 and 4, along with (14), one gets that $\mathbb{P}_{\beta^*}[\mathcal{E}_{\alpha_0}] \le err_{tot}(\alpha_0)$, where

$$err_{\rm tot}(\alpha_0) = \sum_{\ell \ge \alpha_0 L} \min\left\{err_1(\ell/L),\, err_2(\ell/L)\right\}. \qquad (24)$$

This is the bound we use to numerically compute the rate curve in Fig. 2. Accordingly, the error exponent $E(\alpha_0, R)$ of Proposition 1 satisfies

$$E(\alpha_0, R) \ge -\frac{1}{n}\log(err_{\rm tot}(\alpha_0)). \qquad (25)$$

Our task will be to give simplified lower bounds for the right side of (25) for all $R < C$. In the next section, we characterize the section size required to achieve rates up to capacity. In Section V, we prove Proposition 1 and in Section VI, we prove Proposition 2. We also remark that in Appendix F we discuss how the bounds of the aforementioned two lemmas may be modified to deal with the subset superposition coding scheme described in Section I-A.

Since the bounds of Lemma 4 are better than those in Lemma 3 for α values near 1, for simplicity we only use the bounds from Lemma 4 in characterizing the error exponents. Correspondingly, from hereon we take

$$\triangle_\alpha = C_\alpha - \alpha R - t_\alpha, \quad 1-\rho_\alpha^2 = \frac{\alpha(1-\alpha)v}{1+\alpha v} \tag{26}$$

as in Lemma 4.

IV. Sufficient Section Size

We call $a = (\log M)/(\log L)$ the section size rate, that is, the bits required to describe the member of a section relative to the bits required to describe which section. It is invariant to the base of the log. Equivalently, we have M and L related by $M = L^a$. Note that the size of a controls the polynomial size of the dictionary $N = LM = L^{a+1}$.

The code length may be written as

$$n = \frac{aL\log L}{R}.$$

We do not want a requirement on the section sizes with a of order $1/(C-R)$ for then the complexity would grow exponentially with this inverse of the gap from capacity. So, instead, we decompose $\triangle_\alpha = \tilde{\triangle}_\alpha + \alpha(C-R) - t_\alpha$ where $\tilde{\triangle}_\alpha = C_\alpha - \alpha C$. We investigate in this section the use of $\tilde{\triangle}_\alpha$ to cancel out the combinatorial coefficient $\binom{L}{\alpha L}$ appearing in the first term in (23). In subsequent sections, excess in $\tilde{\triangle}_\alpha$, beyond that needed to cancel the combinatorial coefficient, plus $\alpha(C-R)-t_\alpha$ are used to produce exponentially small error probability.

Define $D_{\alpha,v} = D_1(\triangle_\alpha, 1-\rho_\alpha^2)$ and $\tilde{D}_{\alpha,v} = D_1(\tilde{\Delta}_\alpha, 1-\rho_\alpha^2)$. Now, $D_1(\Delta, 1-\rho^2)$ is increasing as a function of Δ, so $D_{\alpha,v}$ is greater than $\tilde{D}_{\alpha,v}$ whenever $\triangle_\alpha > \tilde{\triangle}_\alpha$. Accordingly, we decompose the exponent $D_{\alpha,v}$ as the sum of two components, namely, $\tilde{D}_{\alpha,v}$ and the difference $D_{\alpha,v} - \tilde{D}_{\alpha,v}$.

We then ask whether the first part of the exponent denoted $\tilde{D}_{\alpha,v}$ is sufficient to cancel out the effect of the log combinatorial coefficient $\log\binom{L}{L\alpha}$. That is, we want to arrange for the nonnegativity of the difference

$$d_{n,\alpha} = n\tilde{D}_{\alpha,v} - \log\binom{L}{L\alpha}. \tag{27}$$

This function is plotted in Fig. 3 for specific choices of L, M, v, and R.

Using $n = (aL\log L)/R$, one finds that for sufficiently large a depending on v, the difference $d_{n,\alpha}$ is nonnegative uniformly for the permitted α in $[0,1]$. The smallest such section size rate is

$$a_{v,L} = \max_\alpha \frac{R\log\binom{L}{L\alpha}}{\tilde{D}_{\alpha,v}\, L\log L} \tag{28}$$

where the maximum is for α in $\{1/L, 2/L, \ldots, 1-1/L\}$. This definition is invariant to the choice of base of the logarithm, assuming that the same base is used for the communication rate R and for the $C_\alpha - \alpha C$ that arises in the definition of $\tilde{D}_{\alpha,v}$.

In the aforementioned ratio, the numerator and denominator are both 0 at $\alpha = 0$ and $\alpha = 1$ (yielding $d_{n,\alpha} = 0$ at the ends). Accordingly, we have excluded 0 and 1 from the definition of $a_{v,L}$ for finite L. Nevertheless, limiting ratios arise at these ends.

We give bounds for $a_{v,L}$ and show that the value of $a_{v,L}$ is fairly insensitive to the value of L, with the maximum over the whole range being close to a limit a_v which is characterized by values in the vicinity of $\alpha = 1$.

Let v^* near 15.8 be the solution to $(1+v^*)\log(1+v^*) = 3v^*\log e$.

Lemma 5: The quantity $a_{v,L}$ has the following properties.

(a) For $L > 2$

$$a_{v,L} \le \frac{64R}{(1-\delta_L)}(1+v)^4/v^3 \tag{29}$$

where $\delta_L = \log 2/\log L$.

(b) The limit for large L of $a_{v,L}$ is a continuous function a_v which is given, for $0 < v < v^*$, by

$$\frac{8Rv(1+v)\log e}{[(1+v)\log(1+v) - v\log e]^2} \tag{30}$$

and for $v \ge v^*$ by

$$\frac{2R(1+v)}{[(1+v)\log(1+v) - 2v\log e]}. \tag{31}$$

(c) For all $R \le C$ and using log base e, the a_v aforementioned is bounded by

$$\frac{4v(1+v)\log(1+v)}{[(1+v)\log(1+v) - v]^2} \tag{32}$$

in the case $0 < v < v^*$, which is approximately $16/v^2$ for small positive v, whereas in the case $v \ge v^*$, it is bounded by

$$\frac{(1+v)\log(1+v)}{(1+v)\log(1+v) - 2v} \tag{33}$$

which asymptotes to the value 1 for large v.

The proof of the aforementioned lemma is routine. For convenience, it is given in Appendix B.

While a_v is undesirably large for small v, we have reasonable values for moderately large v. In particular, a_v equals 5.0 and 3, respectively, at $v = 7$ and $v^* = 15.8$, and it is near 1 for large v.

Numerically, it is of interest to ascertain the minimal section size rate $a_{v,L,\epsilon,\alpha_0}$, for a specified L such as $L = 64$, for R chosen to be a given high fraction of C, say $R = 0.8C$, for α_0 at a fixed small target fraction of mistakes, say $\alpha_0 = 0.1$, and for ϵ to be a small target probability, so as to obtain $err_{tot}(\alpha_0) \le \epsilon$. Here, $err_{tot}(\alpha_0)$ as in (24). This is illustrated in Fig. 4 plotting the minimal section size rate as a function of v for $\epsilon = e^{-10}$. With such R moderately less than C, we observe substantial reduction in the required section size rate.

V. Proof of Proposition 1

In this section, we put the aforementioned conclusions together to prove proposition 1, demonstrating the reliability of approximate least squares. The following lemma will be useful in proving the lower bound for the error exponent in proposition 1. Let $g(x) = \sqrt{1+4x^2} - 1$ as earlier.

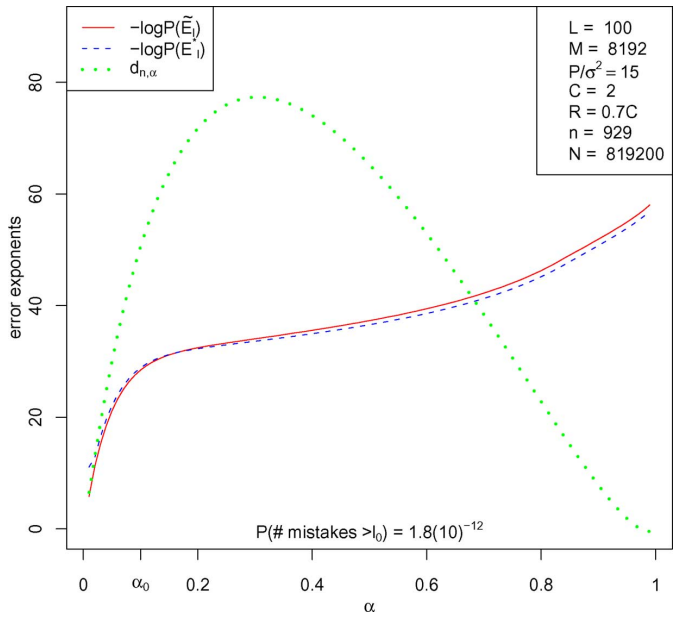

Fig. 3. Exponents of contributions to the error probability as functions of $\alpha = \ell/L$ using exact least squares, i.e., $t = 0$, with $L = 100$, $M = 2^{13}$, signal-to-noise ratio $v = 15$, and rate 70% of capacity. The red and blue curves are the $-\log \mathbb{P}[\tilde{E}_\ell]$ and $-\log \mathbb{P}[E^*_\ell]$ bounds, using the natural logarithm, from the two terms in lemma 4 with optimized t_α. The dotted green curve is $d_{n,\alpha}$ (27). With $\alpha_0 = 0.1$, the total probability of at least that fraction of mistakes is bounded by 1.8×10^{-12}.

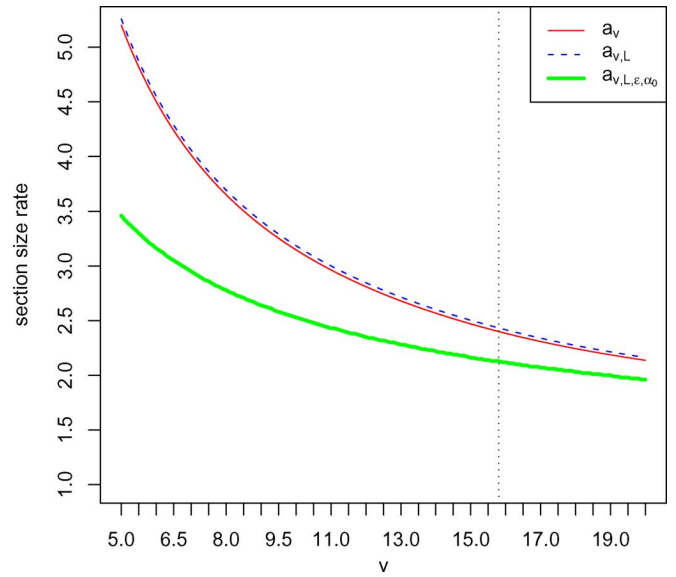

Fig. 4. Sufficient section size rate a as a function of the signal-to-noise ratio v. The dashed curve shows $a_{v,L}$ at $L = 64$. Just below it, the thin solid curve is the limit for large L. For section size $M \geq L^a$, the error probabilities are exponentially small for all $R < C$ and any $\alpha_0 > 0$. The bottom curve shows the minimal section size rate for the bound on the error probability contributions to be less than e^{-10}, with $R = 0.8C$ and $\alpha_0 = 0.1$ at $L = 64$.

Lemma 6: The following bounds hold.

(a) For positive Δ and correlation $\rho \in (0,1)$, let $q = \Delta/\sqrt{1-\rho^2}$. Then

$$D(\Delta, 1-\rho^2) \geq g(q)/4 \tag{34}$$

and

$$D_1(\Delta, 1-\rho^2) \geq \min\{g(q)/4,\, \Delta/2\}\,. \tag{35}$$

(b) For $\alpha \in [0,1]$, let $\tilde{\Delta}_\alpha = C_\alpha - \alpha C$. Then

$$\frac{v^2}{2(1+v)}\alpha(1-\alpha) \geq \tilde{\Delta}_\alpha \geq \frac{v^2}{4(1+v)^2}\alpha(1-\alpha). \tag{36}$$

For convenience, we put its proof in Appendix A.

We now prove Proposition 1. Consider the exponent $D_{\alpha,v} = D_1(\Delta_\alpha, 1-\rho_\alpha^2)$ appearing in the error bound (23). Now, $D_1(\Delta, 1-\rho^2)$ has a nondecreasing derivative with respect to Δ. So $D_{\alpha,v} = D_1(\triangle_\alpha, 1-\rho_\alpha^2)$ is greater than $\tilde{D}_{\alpha,v} = D_1(\tilde{\Delta}_\alpha, 1-\rho_\alpha^2)$. Consequently, it lies above the tangent line (the first order Taylor expansion) at $\tilde{\Delta}_\alpha$, that is

$$D_{\alpha,v} \geq \tilde{D}_{\alpha,v} + (\Delta_\alpha - \tilde{\Delta}_\alpha)\, D' \tag{37}$$

where $D' = D_1'(\Delta)$ is the derivative of $D_1(\Delta) = D_1(\Delta, 1-\rho_\alpha^2)$ with respect to Δ, which is, here, evaluated at $\tilde{\Delta}_\alpha$. In detail, the derivative $D_1'(\Delta)$ is seen to equal

$$\frac{1}{1+\sqrt{1+4\Delta^2/(1-\rho_\alpha^2)}}\,\frac{2\Delta}{1-\rho_\alpha^2} \tag{38}$$

when $\Delta < (1-\rho_\alpha^2)/\rho_\alpha^2$, and this derivative is equal to 1 otherwise. (The latter case with derivative equal to 1 includes the situations $\alpha = 0$ and $\alpha = 1$ where $1-\rho_\alpha^2 = 0$ with $D_1 = \Delta$; all other α have $1-\rho_\alpha^2 > 0$).

We now lower bound the derivative $D' = D_1'(\Delta)$ evaluated at $\Delta = \tilde{\Delta}_\alpha$. Using the upper bound on $\tilde{\Delta}_\alpha$ given in (36) and the form of $1-\rho_\alpha^2$, one gets that $4\tilde{\Delta}_\alpha^2/(1-\rho_\alpha^2)$ is bounded by $[v^3(1+\alpha v)/(1+v)^2]\alpha(1-\alpha)$, which using $1+\alpha v \leq 1+v$ and $\alpha(1-\alpha) \leq 1/4$, one gets that

$$4\tilde{\Delta}_\alpha^2/(1-\rho_\alpha^2) \leq v^3/[4(1+v)].$$

Further using the lower bound in (36), one has $2\tilde{\Delta}_\alpha/(1-\rho_\alpha^2)$ is at least $(1/2)v/(1+v)^2$, where we make use of $1+\alpha v \geq 1$. Correspondingly

$$D_1'(\tilde{\Delta}_\alpha) \geq \frac{v}{[2(1+v)^2]\sqrt{1+(1/4)v^3/(1+v)}} \tag{39}$$

the right side of which is $2w_v$, where w_v is as in (5).

Now, we are in a position to apply lemma 4 and lemma 5. If the section size rate a is at least $a_{v,L}$, we have that $n\tilde{D}_{\alpha,v}$ cancels the combinatorial coefficient $\binom{L}{\alpha L}$, and hence, the first term in the $\mathbb{P}_{\beta^*}[E_\ell]$ bound (23) (the part controlling $\mathbb{P}_{\beta^*}[\tilde{E}_\ell]$) is not more than

$$\exp\{-n[\Delta_\alpha - \tilde{\Delta}_\alpha]\, D'\}$$

where $\alpha = \ell/L$. Using $\Delta_\alpha = C_\alpha - \alpha R - t_\alpha$ and $\tilde{\Delta}_\alpha = C_\alpha - \alpha C$ and (39) yield $\mathbb{P}_{\beta^*}[E_\ell]$ not more than the sum of

$$\exp\{-2w_v n[\alpha(C-R) - t_\alpha]\}$$

and

$$\exp\{-nD(t_\alpha, \alpha^2 v/(1+\alpha^2 v))\}$$

for any choice of $t_\alpha \in [0, \alpha(C–R)]$. For convenience, we take t_α to be $\alpha(C–R)/2$. In this case, the first part of the aforementioned sum is $\exp\{-nw_v\alpha(C-R)\}$.

Now, use (34) to get that $D(t_\alpha, \alpha^2 v/(1+\alpha^2 v))$ is at least $g(q)/4$, where $q = (C-R)\sqrt{1+\alpha^2 v}/(2\sqrt{v})$. Correspondingly, using $(1+\alpha^2 v) \geq 1$, one gets that $q \geq (C-R)/(2\sqrt{v})$. Accordingly, $D(t_\alpha, \alpha^2 v/(1+\alpha^2 v))$ is at least $g((C-R)/(2\sqrt{v}))/4$.

It follows from the aforementioned that

$$\mathbb{P}_{\beta^*}[E_\ell] \leq 2e^{-n\min\left\{\alpha w_v \Delta, \frac{1}{4}g\left(\frac{\Delta}{2\sqrt{v}}\right)\right\}}$$

where $\alpha = \ell/L$, $\Delta = C - R$. Consequently, summing over all $\ell \geq \alpha_0 L$, for which $\alpha \geq \alpha_0$, one gets

$$\mathbb{P}_{\beta^*}[\mathcal{E}_{\alpha_0}] \leq 2Le^{-n\min\left\{\alpha_0 w_v \Delta, \frac{1}{4}g\left(\frac{\Delta}{2\sqrt{v}}\right)\right\}}.$$

The exponent in the right side of the aforementioned equation is $h(\alpha_0, \Delta) - (\log 2L)/n$. Now, use the $\mathbb{P}_{\beta^*}[\mathcal{E}_{\alpha_0}] = \bar{\mathbb{P}}[\mathcal{E}_{\alpha_0}]$ to complete the proof of proposition 1.

Remarks: The form given for the exponential bound is meant only to reveal the general character of what is available. A compromise was made by introduction of an inequality (the tangent bound on the exponent) to proceed most simply to this demonstration. Now, understanding that it is exponentially small, our best evaluation avoids this compromise and proceeds directly, using the bound (24), as it provides substantial numerical improvement.

In the next section, we prove proposition 2, while at the same time review basic properties of the RS codes.

VI. Proof of Proposition 2

We employ RS codes [45], [48], [55] as an outer code for correcting any remaining section mistakes. The symbols for the RS code come from a Galois field consisting of q elements denoted by $GF(q)$, with q typically taken to be of the form 2^m. If K_{out} and n_{out} represent message and codeword lengths, respectively, then an RS code with symbols in $GF(2^m)$ and minimum distance between codewords given by d_{RS} can have the following parameters:

$$n_{out} = 2^m$$
$$n_{out} - K_{out} = d_{\text{RS}} - 1.$$

Here, $n_{\text{out}} - K_{\text{out}}$ gives the number of parity check symbols added to the message to form the codeword. In what follows, we find it convenient to take M to be equal to 2^m so that we can view each symbol in $GF(2^m)$ as giving a number between 1 and M.

We now demonstrate how the RS code can be used as an outer code in conjunction with our inner superposition code to achieve low block error probability. For simplicity, assume that M is a power of 2. First, consider the case when L equals M. Taking $m = \log_2 M$, we have that since L is equal to M, the RS code length becomes L. Thus, one can view each symbol as representing an index in each of the L sections. The number of input symbols is, then, $K_{\text{out}} = L - d_{\text{RS}} + 1$, so setting $\delta = d_{\text{RS}}/L$, one sees that the outer rate R_{out} equals $1 - \delta + 1/L$ which is at least $1 - \delta$.

For code composition, $K_{\text{out}} \log_2 M$ message bits become the K_{out} input symbols to the outer code. The symbols of the outer codeword, having length L, give the labels of terms sent from each section using our inner superposition with code length $n = L(\log_2 M)/R_{\text{inner}}$. From the received Y, the estimated labels $\hat{j}_i, \hat{j}_2, \ldots \hat{j}_L$ using our least squares decoder can be again thought of as output symbols for our RS codes. If $\hat{\delta}_e = mistakes/L$ denotes the section mistake rate, it follows from the distance property of the outer code that if $2\hat{\delta}_e \leq \delta$, then these errors can be corrected. The overall rate R_{comp} is seen to be equal to the product of rates $R_{\text{out}} R_{\text{inner}}$ which is at least $(1-\delta)R_{\text{inner}}$. Since we arrange for $\hat{\delta}_e$ to be smaller than some α_0 with exponentially small probability ϵ, it follows from the previous that composition with an outer code allows us to communicate with the same reliability, albeit with a slightly smaller rate given by $(1 - 2\alpha_0)R_{\text{inner}}$.

The case when $L < M$ can be dealt with by observing ([45], p. 240) that an $(n_{\text{out}}, K_{\text{out}})$ RS code as aforementioned can be shortened by length w, where $0 \leq w < K_{\text{out}}$, to form an $(n_{\text{out}} - w, K_{\text{out}} - w)$ code with the same minimum distance d_{RS} as earlier. This is easily seen by viewing each codeword as being created by appending $n_{\text{out}} - K_{\text{out}}$ parity check symbols to the end of the corresponding message string. Then, the code formed by considering the set of codewords with the w leading symbols identical to zero has precisely the properties stated earlier.

With M equal to 2^m as earlier, we have n_{out} equals M; so taking w to be $M - L$, we get an $(n'_{\text{out}}, K'_{\text{out}})$ code, with $n'_{\text{out}} = L$, $K'_{\text{out}} = L - d_{\text{RS}} + 1$, and minimum distance d_{RS}. Now, since the outer code length is L and symbols of this code are in $GF(M)$, the code composition can be carried out as earlier. This completes the proof of Proposition 2.

VII. Generalization to Approximate Least Squares

In conclusion, we remark that our results are equally valid for an approximate least squares decoder, which for some nonnegative δ_0 chooses a $\hat{\beta} \in \mathcal{B}$ satisfying

$$|Y - X\hat{\beta}|^2 \leq |Y - X\beta^*|^2 + \delta_0 \tag{40}$$

where β^* is what is sent. Since the aforementioned is less restrictive than (2), it may be possible to find a computationally feasible algorithm for it. Indeed, we show in Appendix E that any computationally feasible algorithm, if it be an accurate decoder, then it must be an approximate least squares decoder for some small δ_0.

We now describe how our error probability bounds can be generalized to incorporate (40). We note that (40) is equivalent to finding an $\hat{S} \in \mathcal{A}$, so that $T(\hat{S}) \leq t$, with $t = \delta_0/(2\sigma^2)$, where $T(S)$ is as in (16). We find that the expression for $err_1(\alpha)$ in lemma 3 holds for approximate least squares decoders with $t \leq C_\alpha - \alpha R$, if we replace $\triangle_\alpha$ by $\triangle_\alpha = C_\alpha - \alpha R - t$. Furthermore, the expression for $err_2(\alpha, t_\alpha)$ of lemma 4 is also true for $t \leq C_\alpha - \alpha R$, if one replaces the t_α appearing in the second term of the bound by $t_\alpha - t$. Accordingly, for such approximate

decoders, with $t \le C_\alpha - \alpha R$, the bound corresponding to lemma 4 becomes

$$err_2(\alpha, t_\alpha) = \binom{L}{L\alpha} \exp\left\{-nD_1(\triangle_\alpha, 1-\rho_\alpha^2)\right\} + \exp\left\{-nD(t_\alpha - t, \alpha^2 v/(1+\alpha^2 v)]\right\} \tag{41}$$

where $\triangle_\alpha = C_\alpha - \alpha R - t_\alpha$ and $1-\rho_\alpha^2 = \alpha(1-\alpha)v/(1+\alpha v)$ is as in lemma 4.

The analysis of this decoder is quite similar to that of (2). Interested readers may refer to [11] for a more general analysis incorporating (40).

Appendix A
Proof of Lemma 6

We first prove (a). Write $D(\Delta, 1-\rho^2)$ explicitly as an increasing function of the ratio $q = \Delta/\sqrt{1-\rho^2}$. Working with logarithm base e, the derivative with respect to λ of the expression being maximized yields a quadratic equation which can be solved for the optimal

$$\lambda^* = \frac{1}{2\Delta}\left(\sqrt{1+4\Delta^2/(1-\rho^2)} - 1\right).$$

Using this λ^*, we get that $D = (1/2)\big(\gamma - \log(1+\gamma/2)\big)$, which is at least $\gamma/4$. Here, $\gamma = \sqrt{1+4q^2} - 1$, with $q = \Delta/\sqrt{1-\rho^2}$. Correspondingly, $D(\Delta, 1-\rho^2) \ge g(q)/4$. This proves (34).

For the lower bound on $D_1 = D_1(\Delta, 1-\rho^2)$, recall that the case $\lambda = 1$ case occurs when $1 + 4\Delta^2/(1-\rho^2) \ge (1+2\Delta)^2$, in which case D_1 is at least $\Delta - (1/2)\log(1+\Delta)$. Using $\Delta - (1/2)\log(1+\Delta) \ge \Delta/2$ proves (35).

Next we prove (b). Notice the $\tilde{\Delta}_\alpha$ has second derivative $-(1/2)v^2/(1+\alpha v)^2$. It follows that $\tilde{\Delta}_\alpha \ge (1/4)\alpha(1-\alpha)v^2/(1+v)^2$, since the difference of the two sides has negative second derivative, so it is concave and equals 0 at $\alpha = 0$ and $\alpha = 1$.

For the upper bound, notice that the derivative of Δ_α is v_1 at $\alpha = 0$ and $-v_2$ at $\alpha = 1$, where $v_1 = v/2 - C$ and $v_2 = C - v/[2(1+v)]$. Correspondingly, $\tilde{\Delta}_\alpha$ is bounded from earlier by the minimum of $v_1\alpha$ and $v_2(1-\alpha)$. Now, it is not hard to see that

$$\min\{v_1\alpha,\, v_2(1-\alpha)\} \le \alpha(1-\alpha)(v_1+v_2).$$

Correspondingly, we get the upper bound in (36).

Appendix B
Proof of Lemma 5

We first prove (a). Define $q = \tilde{\Delta}_\alpha/\sqrt{1-\rho_\alpha^2}$, which, using the lower bound on $\tilde{\Delta}_\alpha$ given in lemma 6 (b) and $1-\rho_\alpha^2 = \alpha(1-\alpha)v/(1+\alpha v)$, is at least $(1/4)\sqrt{\alpha(1-\alpha)}v^{3/2}(1+\alpha v)^{1/2}/(1+v)^2$. Consequently, q is at least $(1/4)\sqrt{\alpha(1-\alpha)}v^{3/2}/(1+v)^2$ using $1+\alpha v \ge 1$. Correspondingly, using (35) and the lower bound (7), one gets that $\tilde{D}_{\alpha,v} = D_1(\tilde{\Delta}_\alpha, 1-\rho_\alpha^2)$ is at least

$$\min\left\{\frac{1}{8\sqrt{2}}\frac{\sqrt{\alpha(1-\alpha)}v^{3/2}}{(1+v)^2},\, \frac{\alpha(1-\alpha)v^3}{64(1+v)^4},\, \frac{1}{8}\frac{\alpha(1-\alpha)v^2}{(1+v)^2}\right\}$$

which is equal to $v^{3/2}/[8(1+v)^2]$ times

$$\min\left\{\frac{\sqrt{\alpha(1-\alpha)}}{\sqrt{2}},\, \frac{\alpha(1-\alpha)v^{3/2}}{8(1+v)^2},\, \alpha(1-\alpha)\sqrt{v}\right\}.$$

Furthermore, $\log\binom{L}{L\alpha}$ can be bounded by $\min(\alpha, 1-\alpha)L\log L$ and $L\log 2$. Therefore, it is at most $\alpha(1-\alpha)(L\log L)/(1-\delta_L)$, where $\delta_L = (\log 2)/\log L$. Using this, the lower bound on $\tilde{D}_{\alpha,v}$ and the form of $a_{v,L}$ given in (28), one gets that $a_{v,L}$ can be bounded by $8R(1+v)^2/[(1-\delta_L)v^{3/2}]$ times

$$\max\left\{\sqrt{2\alpha(1-\alpha)},\, \frac{8(1+v)^2}{v^{3/2}},\, 1/\sqrt{v}\right\}.$$

Now, use $\alpha(1-\alpha) \le 1/4$ to get that

$$a_{v,L} \le \frac{8R(1+v)^2}{(1-\delta_L)v^{3/2}} \max\left\{1/\sqrt{2},\, \frac{8(1+v)^2}{v^{3/2}},\, 1/\sqrt{v}\right\}.$$

Now, observe that the second term in the maximum given previously dominates the other two terms for all v. This completes the proof of (a).

Next we prove (b). For α in $(0,1)$, we use $\log\binom{L}{L\alpha} \le L\log 2$ and the strict positivity of $\tilde{D}_{\alpha,v}$ to see that the ratio in the definition of $a_{v,L}$ tends to zero uniformly within compact sets interior to $(0,1)$. So the limit a_v is determined by the maximum of the limits of the ratios at the two ends. In the vicinity of the left and right ends, we replace $\log\binom{L}{L\alpha}$ by the continuous upper bounds $\alpha L\log L$ and $(1-\alpha)L\log L$, respectively, which are tight at $\alpha = 1/L$ and $1-\alpha = 1/L$, respectively. Then, in accordance with L'Hôpital's rule, the limit of the ratios equals the ratios of the derivatives at $\alpha = 0$ and $\alpha = 1$, respectively. Accordingly

$$a_v = \max\left\{\frac{R}{\tilde{D}'_{0,v}}, \frac{-R}{\tilde{D}'_{1,v}}\right\} \tag{42}$$

where $\tilde{D}'_{0,v}$ and $\tilde{D}'_{1,v}$ are the derivatives of $\tilde{D}_{\alpha,v}$ with respect to α evaluated at $\alpha = 0$ and $\alpha = 1$, respectively.

To determine the behavior of $\tilde{D}_\alpha = \tilde{D}_{\alpha,v}$ in the vicinity of 0 and 1, we first need to determine whether the optimal λ in its definition is strictly less than 1 or equal to 1. From Section II, the case $\lambda < 1$ occurs if and only if $\tilde{\Delta}_\alpha < (1-\rho_\alpha^2)/\rho_\alpha^2$. The right side of this is $\alpha(1-\alpha)v/(1+\alpha^2 v)$. So it is equivalent to determine whether the ratio

$$\frac{(C_\alpha - \alpha C)(1+\alpha^2 v)}{\alpha(1-\alpha)v}$$

is less than 1 for α in the vicinity of 0 and 1. Using L'Hôpital's rule, it suffices to determine whether the ratio of derivatives is less than 1 when evaluated at 0 and 1. At $\alpha = 0$, it is $(1/2)[v - \log(1+v)]/v$ which is not more than 1/2 (certainly less than 1) for all positive v, whereas at $\alpha = 1$, the ratio of derivatives is $(1/2)[(1+v)\log(1+v) - v]/v$ which is less than 1 if and only

if $v < v^*$. In other words, at $\alpha = 0$, the optimum λ is less than one for all v, whereas at $\alpha = 1$, it is less than one if and only if $v < v^*$.

For the cases in which the optimal $\lambda < 1$, we need to determine the derivative of $\tilde{D}_\alpha$ at $\alpha=0$ and $\alpha=1$. Recall that $\tilde{D}_\alpha$ is the composition of the functions $(1/2)(\gamma - \log(1+\gamma/2))$ and $\gamma = \sqrt{1+q} - 1$ and $q = q_\alpha = 4\tilde{\Delta}_\alpha^2/(1-\rho_\alpha^2)$. Also recall that the limit of q_α, as α tends to 0 or 1, is zero.

Use chain rule for finding the derivative of $\tilde{D}_\alpha$, taking the products of the associated derivatives. The first of these functions has derivative $(1/2)(1-1/(2+\gamma))$ which is 1/4 at $\gamma=0$, the second of these has derivative $1/(2\sqrt{1+u})$ which is 1/2 at $u=0$, and the third of these functions is

$$u_\alpha = \frac{\big(\log(1+\alpha v) - \alpha\log(1+v)\big)^2}{\alpha(1-\alpha)v/(1+\alpha v)}$$

which has derivative that evaluates to $(v-\log(1+v))^2/v$ at $\alpha = 0$ and evaluates to $-[(1+v)\log(1+v) - v]^2/[v(1+v)]$ at $\alpha = 1$. Correspondingly, for $\alpha = 0$, the derivative of $\tilde{D}_\alpha$ is $(v-\log(1+v))^2/(8v)$ for all v, whereas for $\alpha = 1$, its derivative is $-[(1+v)\log(1+v) - v]^2/[8v(1+v)]$ for $v < v^*$.

For $v < v^*$, the magnitude of the derivative of $\tilde{D}_\alpha$ at 1 is smaller than at 0. Indeed, taking square roots, this is the same as the claim that $(1+v)\log(1+v) - v < \sqrt{1+v}(v - \log(1+v))$. Replacing $s = \sqrt{1+v}$ and rearranging, it reduces to $s\log s < (s^2-1)/2$, which is true for $s>1$ since the two sides match at $s = 1$ and have derivatives $1 + \log s < s$. Thus, the limiting value for α near 1 is what matters for the maximum. This produces the claimed form of a_v for $v < v^*$.

In contrast for $v > v^*$, the optimal λ equals 1 for α in the vicinity of 1. In this case, we use $\tilde{D}_\alpha = \tilde{\Delta}_\alpha + (1/2)\log\rho_\alpha^2$ which has derivative equal to $-(1/2)[(1+v)\log(1+v) - 2v]/(1+v)$ at $\alpha=1$, which is again smaller in magnitude than the derivative at $\alpha=0$, producing the claimed form for a_v for $v > v^*$.

At $v = v^*$ we equate $(1+v)\log(1+v) = 3v$ and see that both of the expressions for the magnitude of the derivative at 1 agree with each other (both reducing to $v^*/(2(1+v^*))$), so the argument extends to this case, and the expression for a_v is continuous in v.

(c) is proved by using $R \le (1/2)\log(1+v)$ and simplifying the resulting expression. This completes the proof of Lemma 5.

Appendix C
Improvement in Form of Exponent

The following improvement in the form of the exponent in Proposition 1 can be obtained.

Theorem 7: Assume $M = L^a$, where $a \ge a_{v,L}$, and rate R is less than capacity C. For the least squares decoder

$$\bar{\mathbb{P}}[\mathcal{E}_{\alpha_0}] \le 2Le^{-n\tilde{h}(\alpha_0, C-R)}.$$

Here

$$\tilde{h}(\alpha_0, C-R) = \min\left\{c_{\alpha_0,v}\,\alpha_0,\ \frac{1}{4}g\left(\frac{C-R}{2\sqrt{v}}\right)\right\}$$

where $c_{\alpha,v}$ is positive and tends to $\tau_v\tilde{w}_v/4$ as α tends to 0. Here

$$\tau_v = (1/2)[v - \log(1+v)] - [2vR/a]^{1/2} \tag{43}$$

and

$$\tilde{w}_v = (v/2 - C)/(2v). \tag{44}$$

Proof of Theorem 7: Here, we determine the minimum value of Δ for which the combinatorial term $\binom{L}{L\alpha}$ is canceled, and we characterize the amount beyond that minimum which makes the error probability exponentially small. Arrange $\Delta_\alpha^{\min}$ to be the solution to the equation

$$nD_1(\Delta_\alpha^{\min}, 1-\rho_\alpha^2) = \log\binom{L}{L\alpha}.$$

To see its characteristics, let $\Delta_\alpha^{\text{target}} = (1-\rho_\alpha^2)^{1/2}G(r_\alpha)$ at

$$r_\alpha = \frac{1}{n}\log\binom{L}{L\alpha}$$

using log base e. Here, $G(r)$ is the inverse of the function $D(\delta, 1)$ which is the composition of the increasing functions $(1/2)[\gamma - \log(1+\gamma/2)]$ and $\gamma = \sqrt{1+4\delta^2} - 1$ previously discussed in Section II. This $G(r)$ is near $\sqrt{2r}$ for small r. When $G(r) < (1-\rho_\alpha^2)^{1/2}/\rho_\alpha^2$, the condition $\lambda < 1$ is satisfied and $\Delta_\alpha^{\min} = \Delta_\alpha^{\text{target}}$ indeed solves the aforementioned equation; otherwise, $\Delta_\alpha^{\min} = r_\alpha - (1/2)\log\rho_\alpha^2$ provides the solution.

Now, $r_\alpha = (R/a)(\log\binom{L}{\alpha L})/(L\log L)$, which from earlier can be bounded by $(R/a)\alpha(1-\alpha)/(1-\delta_L)$. Also, $1-\rho_\alpha^2 = \alpha(1-\alpha)v/(1+\alpha v)$. Consequently, $\Delta_\alpha^{\min}$ is small for large L; moreover, for α near 0 and 1, it is of order α and $1-\alpha$, respectively, and via the indicated bounds, derivatives at 0 and 1 can be explicitly determined.

The analysis in Lemma 5 may be interpreted as determining section size rates a such that the differentiable upper bounds on $\Delta_\alpha^{\min}$ are less than or equal to $\tilde{\Delta}_\alpha = C_\alpha - \alpha C$ for $0 \le \alpha \le 1$, where, noting that these quantities are 0 at the endpoints of the interval, the critical section size rate is determined by matching the slopes at $\alpha = 1$. At the other end of the interval, the bound on the difference $\tilde{\Delta}_\alpha - \Delta_\alpha^{\min}$ has a strictly positive slope for $a \ge a_v$ at $\alpha = 0$, given by τ_v as in (43). The positivity of τ_v follows from recalling that $a_v > R/\tilde{D}'_{0,v}$, since the second term in (42) always turns out to be the greater one. Consequently, one may take $\tilde{\Delta}_\alpha - \Delta_\alpha^{\min} = \tau_{\alpha,v}\,\alpha$ for some positive $\tau_{\alpha,v}$, where $\tau_{\alpha,v}$ tends to τ_v as α tends to 0.

Recall that $\Delta_\alpha = C_\alpha - \alpha R - t_\alpha$. Express Δ_α as the sum of $\Delta_\alpha^{\min}$ needed to cancel the combinatorial coefficient, and $\Delta_\alpha^{\text{extra}} = C_\alpha - \alpha R - \Delta_\alpha^{\min} - t_\alpha$, which is positive. This $\Delta_\alpha^{\text{extra}}$ arises in establishing that the main term in the probability bound is exponentially small. It decomposes as $\Delta_\alpha^{\text{extra}} = \alpha(C-R) + (\tilde{\Delta}_\alpha - \Delta_\alpha^{\min}) - t_\alpha$. Arrange t_α to be $(1/2)[\alpha(C-R) + \tilde{\Delta}_\alpha - \Delta_\alpha^{\min}]$ so that $\Delta_\alpha^{\text{extra}} = (1/2)[\alpha(C-R) + \tau_{\alpha,v}\alpha]$.

Consider the exponent $D_{\alpha,v} = D_1(\Delta_\alpha, 1-\rho_\alpha^2)$ as given in lemma 4. We take a reference $\Delta_\alpha^{\text{ref}}$ for which $\Delta_\alpha > \Delta_\alpha^{\text{ref}}$ and for which $\Delta_\alpha^{\text{ref}}$ is at least $\Delta_\alpha^{\min}$ and at least a multiple of $\tilde{\Delta}_\alpha$. For convenience, we set $\Delta_\alpha^{\text{ref}} = (1/2)[\Delta_\alpha + \Delta_\alpha^{\min}]$ to

be half way between $\Delta_\alpha^{\min}$ and Δ_α. Recall that $D_1(\Delta, 1-\rho^2)$ has a nondecreasing derivative with respect to Δ. So $D_{\alpha,v} = D_1(\triangle_\alpha, 1-\rho_\alpha^2)$ is greater than $D_{\alpha,v}^{\text{ref}} = D_1(\Delta_\alpha^{\text{ref}}, 1-\rho_\alpha^2)$. Consequently, it lies above the tangent line at $\Delta_\alpha^{\text{ref}}$, that is

$$D_{\alpha,v} \geq D_{\alpha,v}^{\text{ref}} + (\Delta_\alpha - \Delta_\alpha^{ref})\, D'$$

where as earlier $D' = D_1'(\Delta)$ is the derivative of $D_1(\Delta) = D_1(\Delta, 1-\rho_\alpha^2)$ with respect to Δ, which is, here, evaluated at $\Delta_\alpha^{\text{ref}}$. Its expression is as in (38).

We wish to examine the behavior of $D_1'(\Delta_\alpha^{\text{ref}})$ for α near 0. For this, we first lower bound the derivative $D_1'(\Delta_\alpha^{\text{ref}})$. Since this derivative is nondecreasing, it is at least as large as the value at $\Delta = (1/4)\tilde{\Delta}_\alpha$. Now, recall that $\tilde{\Delta}_\alpha^2/(1-\rho_\alpha^2)$ has a limit 0 as α tends to 0. Furthermore, $\tilde{\Delta}_\alpha/(1-\rho_\alpha^2)$ has limit $(v/2-C)/v$ as α tends to 0. Consequently, from (38), at $\Delta = (1/4)\tilde{\Delta}_\alpha$, we have $D_1'(\Delta)$ tends to $\tilde{w}_v$, given by (44), as α tends to 0. Consequently, $D_1'(\Delta_\alpha^{\text{ref}}) \geq \tilde{w}_{\alpha,v}$, where $\tilde{w}_{\alpha,v}$ is positive and tends to $\tilde{w}_v$ as α goes to 0.

Next examine $D_{\alpha,v}^{\text{ref}}$. Since $\Delta_\alpha^{\text{ref}}$ is at least $\Delta_\alpha^{\min}$, it follows that $D_{\alpha,v}^{\text{ref}}$ is at least $D_{\alpha,v}^{\min} = D(\Delta_\alpha^{\min}, 1-\rho_\alpha^2)$. Consequently, as in the proof of proposition 1, if the section size rate a is at least $a_{v,L}$, then the $\mathbb{P}_{\beta^*}[E_\ell]$ bound (23) is not more than the sum of

$$\exp\{-n[\Delta_\alpha - \Delta_\alpha^{\text{ref}}]\, D'\}$$

and

$$\exp\{-nD(t_\alpha, \alpha^2 v/(1+\alpha^2 v))\}.$$

Using $\Delta_\alpha^{\text{ref}}$ half way between $\Delta_\alpha^{\min}$ and Δ_α, the first part of the bound is at most

$$\exp\{-n(1/4)[\alpha(C-R) + \tau_{\alpha,v}\alpha]\, \tilde{w}_{\alpha,v}\}.$$

This bound is superior to the previous one, when R closely matches C, because of the addition of the nonnegative $\tau_{\alpha,v}\alpha$ term. The second part of the bound can be dealt with as in proposition 1. Accordingly, we have proved that

$$\bar{\mathbb{P}}[\mathcal{E}_{\alpha_0}] \leq 2Le^{-n\min\left\{c_{\alpha_0,v}\,\alpha_0,\, \frac{1}{4}g\left(\frac{C-R}{2\sqrt{v}}\right)\right\}}$$

where $c_{\alpha,v} = \tau_{\alpha,v}\tilde{w}_{\alpha,v}/4$ for small α. It tends to $\tau_v\tilde{w}_v/4$ as α tends to 0. This completes the proof of Theorem 7.

Appendix D
Computations

We describe how the rate curves in Fig. 2 were computed. The block error probability ϵ was fixed at 10^{-4} and the signal-to-ratio v was taken to be 20 and 100. The PPV curve was curve was computed using the right side of (8) for the given ϵ and v. The maximum achievable (composite) rate for the superposition code was calculated in the following manner. The number of sections, L ranged from 20 to 100 in steps of 10, with the corresponding section size M taken to be L^{a_v}, where a_v as in (32) and (33).

For given ϵ and values of v, L, and M, the inner coder rate R_{inner} was decreased from $.99C$ to $.05C$ in decrements of $.001C$. For a given R_{inner}, the minimum section mistake rate $\alpha(R_{\text{inner}})$ so that the error probability, computed using bounds (24), is at most ϵ was computed. The corresponding composite rate is taken to be

$$R_{\text{comp}}(R_{\text{inner}}) = (1 - 2\alpha(R_{\text{inner}}))R_{\text{inner}}.$$

The maximum of the composite rates $R_{\text{comp}}(R_{\text{inner}})$, when R_{inner} ranged from $.99C$ to $.05C$ in decrements of $.001C$, is the reported maximum achievable rate for the superposition code for the given values of ϵ, v, L, and M.

Appendix E
Accurate Decoder ⇒ Approximate Least Squares

In Lemma 9 in the following, we show that any decoder is an approximate least squares decoder. More specifically, we show that if the fraction of mistakes α made by a decoder is small, the distance of the estimated fit $X\hat{\beta}$ from Y cannot be much greater than distance of the codeword sent, that is $X\beta^*$, from Y. To prove this, we require the following lemma, which is a consequence of the restricted isometry property [16], [17] for Gaussian random matrices. We recall that the entries of our X matrix are i.i.d $N(0, P/L)$.

Lemma 8: Let $R < C$ and $n = (L\log M)/R$. Then, the following holds except on a set with probability at most $e^{-n(C-R)}$:

$$|X\beta - X\beta'| \leq c_{\text{rip}}\frac{\|\beta - \beta'\|}{\sqrt{L}} \quad \text{for all} \quad \beta,\, \beta' \in \mathcal{B} \tag{45}$$

where $c_{\text{rip}} = \sqrt{P}(1 + \sqrt{C/\log M} + \sqrt{2C})$ is related to the restricted isometry property constant.

Proof: Statement (45) is equivalent to giving uniform bounds on the maximum singular value of the matrices $W_S = X_S/\sqrt{n}$, for all $S \in \mathcal{A}$, where $\mathcal{A}$ is as in (13). For $S \in \mathcal{A}$, let $\lambda(W_S)$ denote the maximum singular value of W_S. We use a result in [61] (see also [17]), giving tail bounds for the maximum singular value for Gaussian matrices from which one gets that for positive r

$$\mathbb{P}[\lambda(W_S) > 1 + \sqrt{L/n} + r] \leq e^{-nr^2/2}.$$

Accordingly, choose $r = \sqrt{2C}$ and use $\sqrt{L/n} \leq \sqrt{C/\log M}$ to get that $\lambda(W_S) \leq c_{\text{rip}}$, except on a set with probability e^{-nC}.

We need $\lambda(W_S) \leq c_{\text{rip}}$ to hold uniformly for all M^L sets $S \in \mathcal{A}$, with high probability. Correspondingly, using $M^L = e^{nR}$, using a union bound, one gets that the probability of the event

$$\lambda(W_S) \leq c_{\text{rip}} \quad \text{for all} \quad S \in \mathcal{A}$$

is at least $1 - e^{-n(C-R)}$. This completes the proof of the lemma.

If $\epsilon \sim N_n(0, \sigma^2)$, then from standard results on the tail bounds of chi-square random variables, one has that

$$\mathbb{P}[|\epsilon| > 2\sigma] \leq e^{-n/2}. \tag{46}$$

Lemma 8 and (46) gives us the following.

Lemma 9: Assume that a decoder for the superposition code, operating at rate $R < C$, makes at most α section of mistakes. Denote as $\hat{\beta}$ the estimate of the true β^* outputted by the decoder. Then, with probability at least $1 - 2e^{-n\min\{(C-R),1/2\}}$, the estimate $\hat{\beta}$ satisfies

$$|Y - X\hat{\beta}|^2 \le |Y - X\beta^*|^2 + \delta_0$$

with $\delta_0 = c_{\rm rip}\left(4\sqrt{2}\sigma + 2c_{\rm rip}\sqrt{\alpha}\right)\sqrt{\alpha}$. In other words, with high probability, $\hat{\beta}$ is the solution of an approximate least squares decoder (40) with the given δ_0.

Proof: We need to show that $|Y - X\hat{\beta}|^2$ cannot be much greater than $|Y - X\beta^*|^2$. Notice that

$$\begin{aligned} |Y - X\hat{\beta}|^2 &\le \Big(|Y - X\beta^*| + |X\hat{\beta} - X\beta^*|\Big)^2 \\ &= |Y - X\beta^*|^2 + 2|\epsilon||X\hat{\beta} - X\beta^*| \\ &\quad + |X\hat{\beta} - X\beta^*|^2 \end{aligned} \tag{47}$$

where for (47) we use the fact that the noise $\epsilon = Y - X\beta^*$. Now, $\|\hat{\beta} - \beta^*\|^2/L \le 2\alpha$, since the decoder makes at most α mistakes. Accordingly, using lemma 8 and (46), one gets that with probability at least $1 - 2e^{-n\min\{(C-R),1/2\}}$, one gets that $|X\hat{\beta} - X\beta^*| \le c_{\rm rip}\sqrt{2}\sqrt{\alpha}$ and $|\epsilon| \le 2\sigma$. Consequently, from (47), one gets

$$|Y - X\hat{\beta}|^2 \le |Y - X\beta^*|^2 + \delta_0$$

with probability at least $1 - 2e^{-n\min\{(C-R),1/2\}}$, where $\delta_0 = c_{\rm rip}\left(4\sqrt{2}\sigma + 2c_{\rm rip}\sqrt{\alpha}\right)\sqrt{\alpha}$.

APPENDIX F
ERROR BOUNDS FOR SUBSET SUPERPOSITION CODES

The method of analysis also allows the consideration of subset superposition coding described in Section I-A. In this case, all $\binom{N}{L}$ subsets of size L correspond to codewords, so with the rate in nats, we have $e^{nR} = \binom{N}{L}$. The analysis proceeds in the same manner, with the same number $\binom{L}{L-\ell}$ of choices of sets $S_1 = S \cap S^*$ where S and S^* agree on $L - \ell$ terms, but now with $\binom{N-L}{\ell}$ choices of sets $S_2 = S - S^*$ of size ℓ they disagree. We obtain the same bounds as earlier except that where we have $M^\ell = e^{n\alpha R}$, with the exponent αR, it is replaced by $\binom{N-L}{\ell} = e^{nR(\alpha)}$, with the exponent $R(\alpha)$ defined by $R(\alpha) = R\log\binom{N-L}{\alpha L}/\log\binom{N}{L}$.

Correspondingly, for subset superposition coding, the probability $P_{\beta^*}[E_\ell]$ is bounded by the minimum of the same expressions given in Lemma 3 and Lemma 4, except that the term αR appearing in these expression is replaced by the quantity $R(\alpha)$ defined previously. We have not investigated in greater detail for whether there is reliability for any rate below capacity for these codes.

ACKNOWLEDGMENT

We thank John Hartigan, Cong Huang, Yiannis Kontiyiannis, Mokshay Madiman, Xi Luo, Dan Spielman, Edmund Yeh, John Hartigan, Mokshay Madiman, Dan Spielman, Imre Teletar, Harrison Zhou, David Smalling, and Creighton Heaukulani for helpful conversations.

REFERENCES

[1] A. Abbe and A. R. Barron, "Polar coding schemes for the AWGN channel," in *Proc. IEEE Int. Symp. Inf. Theory*, St. Petersburg, Russia, Aug. 2011, pp. 194–198.
[2] M. Akcakaya and V. Tarokh, "Shannon-theoretic limits on noisy compressive sampling," *IEEE Trans. Inf. Theory*, vol. 56, no. 1, pp. 492–504, Jan. 2010.
[3] E. Arikan, "Channel polarization," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, Jul. 2009.
[4] E. Arikan and E. Telatar, "On the rate of channel polarization," in *Proc. IEEE Int. Symp. Inf. Theory*, Seoul, Korea, Jul. 2009, pp. 1493–1495.
[5] A. Barg and G. Zémor, "Error exponents of expander codes under linear-complexity decoding," *SIAM J. Discrete Math.*, vol. 17, no. 3, pp. 426–445, 2004.
[6] A. R. Barron, "Universal approximation bounds for superpositions of a sigmoidal function," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 930–944, May 1993.
[7] A. Barron, A. Cohen, W. Dahmen, and R. Devore, "Approximation and learning by greedy algorithms," *Ann. Statist.*, vol. 36, no. 1, pp. 64–94, 2007.
[8] A. R. Barron and A. Joseph, Sparse superposition codes: Fast and reliable at rates approaching capacity with Gaussian noise [Online]. Available: http://www.stat.yale.edu/arb4
[9] A. R. Barron and A. Joseph, "Towards fast reliable communication at rates near capacity with Gaussian noise," in *Proc. IEEE. Int. Symp. Inf. Theory*, Austin, TX, Jun. 13–18, 2010, pp. 315–319.
[10] A. R. Barron and A. Joseph, "Least squares superposition codes of moderate dictionary size, reliable at rates up to capacity," in *Proc. IEEE. Int. Symp. Inf. Theory*, Austin, TX, Jun. 13–18, 2010, pp. 275–279.
[11] A. R. Barron and A. Joseph, Least squares superposition codes of moderate dictionary size, reliable at rates up to capacity [Online]. Available: http://arxiv.org/abs/1006.3780
[12] G. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding: turbo codes," in *Proc. Int. Conf. Commun.*, Geneva, Switzerland, May 1993, pp. 1064–1070.
[13] T. Blumensath and M. E. Davies, "Iterative thresholding for sparse approximations," *J. Fourier Anal. Appl.*, vol. 14, pp. 629–654, 2008.
[14] L. Applebaum, W. U. Bajwa, M. F. Duarte, and R. Calderbank, "Multiuser detection in asynchronous on-off random access channels using lasso," in *Proc. 48th Annu. Allerton Conf. Commun., Control, Comput.*, Sep. 2010, pp. 130–137.
[15] E. Candes and Y. Plan, "Near-ideal model selection by ℓ_1 minimization," *Ann. Statist.*, vol. 37, no. 5A, pp. 2145–2177, 2009.
[16] E. Candes and T. Tao, "Decoding by linear programming," *IEEE Trans. Inf. Theory*, vol. 51, no. 12, pp. 4203–4215, Dec. 2005.
[17] E. Candes and T. Tao, "Near-optimal signal recovery from random projections: Universal encoding strategies?," *IEEE Trans. Inf. Theory*, vol. 52, no. 12, pp. 5406–5425, Dec. 2006.
[18] J. Cao and E. M. Yeh, "Asymptotically optimal multiple-access communication via distributed rate splitting," *IEEE Trans. Inf. Theory*, vol. 53, no. 1, pp. 304–319, Jan. 2007.
[19] T. M. Cover, "Broadcast channels," *IEEE Trans. Inf. Theory*, vol. 18, no. 1, pp. 2–14, Jan. 1972.
[20] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York: Wiley-Interscience, 2006.
[21] I. Daubechies, M. Defrise, and C. De Mol, "An iterative thresholding algorithm for linear inverse problems with a sparsity constraint," *Commun. Pure Appl. Math.*, vol. 57, no. 11, pp. 1413–1457, 2004.
[22] D. Donoho, "For most large underdetermined systems of linear equations the minimal ℓ^1-norm near solution approximates the sparest solution," *Commun. Pure Appl. Math.*, vol. 59, no. 10, pp. 907–934, 2006.
[23] D. L. Donoho, M. Elad, and V. M. Temlyakov, "Stable recovery of sparse overcomplete representations in the presence of noise," *IEEE Trans. Inf. Theory*, vol. 52, no. 1, pp. 6–18, Jan. 2006.
[24] D. Donoho and X. Huo, "Uncertainty principles and ideal atomic decomposition," *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 2845–2862, Nov. 2001.

[25] D. L. Donoho and J. Tanner, "Exponential bounds implying construction of compressed sensing matrices, error-correcting codes, and neighborly polytopes by random sampling," *IEEE Trans. Inf. Theory*, vol. 56, no. 4, pp. 2002–2016, Apr. 2010.

[26] P. Elias, "Coding for noisy channels," in *IRE Conv. Rec.*, Mar. 1955, pp. 37–46.

[27] A. K. Fletcher, S. Rangan, and V. K. Goyal, On-off random access channels: A compressed sensing framework 2009 [Online]. Available: arXiv:0903.1022v2

[28] A. K. Fletcher, S. Rangan, V. K. Goyal, and K. Ramchandran, "Denoising by sparse approximation: Error bounds based on rate-distortion theory," *J. Appl. Signal Process.*, vol. 10, pp. 1–19, 2006.

[29] A. K. Fletcher, S. Rangan, and V. K. Goyal, "Necessary and sufficient conditions on sparsity pattern recovery," *IEEE Trans. Inf. Theory*, vol. 55, no. 12, pp. 5758–5772, Dec. 2009.

[30] G. D. Forney Jr., *Concatenated Codes*. Cambridge, MA: MIT Press, 1966, vol. 37, Research Monograph.

[31] G. D. Forney Jr. and G. Ungerboeck, "Modulation and coding for linear Gaussian channels," *IEEE Trans. Inf. Theory*, vol. 44, no. 6, pp. 2384–2415, Oct. 1998.

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

[33] J. J. Fuchs, "Recovery of exact sparse representations in the presence of noise," in *Proc. Int. Conf. Acoust., Speech Signal Process.*, Montreal, QC, Canada, 2004, vol. 2, pp. 533–536.

[34] R. G. Gallager, *Low Density Parity-Check Codes*. Cambridge, MA: MIT Press, 1963.

[35] R. G. Gallager, *Information Theory and Reliable Communication*. New York: Wiley, 1968.

[36] A. C. Gilbert and J. A. Tropp, "Applications of sparse approximation in communications," in *Proc. IEEE. Int. Symp. Inf. Theory*, Adelaide, Australia, Sep. 2005, pp. 1000–1004.

[37] C. He, M. Lentmaier, D. J. Costello, and K. S. Zigangirov, "Joint permutor analysis and design for multiple turbo codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 4068–4083, Sep. 2006.

[38] C. Huang, A. R. Barron, and G. H. L. Cheang, Risk of penalized least squares, greedy selection and L1 penalization for flexible function libraries 2008 [Online]. Available: http://www.stat.yale.edu/arb4

[39] W. Hoeffding, "Probability inequalities for sums of bounded random variables," *J. Amer. Statist. Assoc.*, vol. 58, pp. 13–30, Mar. 1963.

[40] J. X. Hu, H. Zhao, and H. H. Zhou, "False discovery rate control with groups," *J. Amer. Statist. Assoc.*, vol. 105, pp. 1215–1227, Sep. 2010.

[41] L. Jones, "A simple lemma for optimization in a Hilbert space, with application to projection pursuit and neural net training," *Ann. Statist.*, vol. 20, pp. 608–613, 1992.

[42] I. Kontoyiannis, S. Gitzenis, and K. R. Rad, "Superposition codes for Gaussian vector quantization," in *IEEE Inf. Theory Workshop*, Cairo, Egypt, Jan. 2010.

[43] A. M. Kakhaki, H. K. Abadi, P. Pad, H. Saeedi, K. Alishahi, and F. Marvasti, Capacity achieving random sparse linear codes 2011 [Online]. Available: arXiv:1102.4099v1

[44] W. S. Lee, P. Bartlett, and B. Williamson, "Efficient agnostic learning of neural networks with bounded fan-in," *IEEE Trans. Inf. Theory*, vol. 42, no. 6, pp. 2118–2132, Nov. 1996.

[45] S. Lin and D. Costello, *Error Control Coding: Fundamentals and Applications*. Englewood Cliffs, NJ: Prentice-Hall, 2004.

[46] M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi, and D. A. Spielman, "Efficient erasure correcting codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 569–584, Feb. 2001.

[47] M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi, and D. A. Spielman, "Improved low-density parity-check codes using irregular graphs," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 585–598, Feb. 2001.

[48] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North Holland, 1981.

[49] S. Mallat and Z. Zhang, "Matching pursuit with time-frequency dictionaries," *IEEE Trans. Signal Process.*, vol. 41, no. 12, pp. 3397–3415, Dec. 1993.

[50] R. J. McEliece, D. J. C. MacKay, and J. F. Cheng, "Turbo decoding as an instance of Pearl's belief propagation algorithm," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 2, pp. 140–152, Feb. 1998.

[51] D. Needell and J. Tropp, "CoSaMP: Iterative signal recovery from incomplete and inaccurate samples," *Appl. Comput. Harmon. Anal.*, vol. 26, no. 3, pp. 301–321, 2009.

[52] Y. C. Pati, R. Rezaiifar, and P. S. Krishnaprasad, "Orthogonal matching pursuit: Recursive function approximation with applications to wavelet decomposition," in *Proc. 27th Annu. Asilomar Conf. Signals, Syst., Comput.*, Pacific Grove, CA, Nov. 1993, pp. 40–44.

[53] Y. Polyanskiy, H. V. Poor, and S. Verdu, "Channel coding rate in the finite block length regime," *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2307–2359, May 2010.

[54] L. Perez, J. Seghers, and D. J. Costello Jr., "A distance spectrum interpretation of turbo codes," *IEEE Trans. Inf. Theory*, vol. 42, no. 6, pp. 1698–1709, Nov. 1996.

[55] I. S. Reed and G. Solomon, "Polynomial codes over certain finite fields," *J. SIAM*, vol. 8, pp. 300–304, Jun. 1960.

[56] G. Reeves and M. Gastpar, "Sampling bounds for sparse support recovery in the presence of noise," in *Proc. IEEE Int. Symp. Inf. Theory*, Toronto, ON, Canada, Jul. 2008, pp. 2187–2191.

[57] T. Richardson, A. Shokrollahi, and R. Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 619–637, Feb. 2001.

[58] T. Richardson and R. Urbanke, "The capacity of low-density parity check codes under message-passing decoding," *IEEE Trans. Inform. Theory*, vol. 47, no. 2, pp. 599–618, Feb. 2001.

[59] B. Rimoldi and R. Urbanke, "A rate-splitting approach to the Gaussian multiple-access channel capacity," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 364–375, Mar. 2001.

[60] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, pp. 379–423, 1948.

[61] S. J. Szarek, "Condition numbers of random matrices," *J. Complexity*, vol. 7, pp. 131–149, 1991.

[62] R. Tibshirani, "Regression shrinkage and selection via the lasso," *J. Roy. Statist. Soc.*, ser. B, vol. 58, no. 1, pp. 267–288, 1996.

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

[64] J. Tropp, "Just relax: Convex programming methods for identifying sparse signals in noise," *IEEE Trans. Inf. Theory*, vol. 52, no. 3, pp. 1030–1051, Mar. 2006.

[65] J. A. Tropp, "On the conditioning of random subdictionaries," *Appl. Comput. Harmon. Anal.*, vol. 25, pp. 1–24, 2008.

[66] J. A. Tropp, "Norms of random submatrices and sparse approximation," *C. R. Math. Acad. Sci. Paris*, vol. 346, no. 23, pp. 1271–1274, 2008.

[67] M. J. Wainwright, "Information-theoretic limits on sparsity recovery in the high-dimensional and noisy setting," *IEEE Trans. Inf. Theory*, vol. 55, no. 12, pp. 5728–5741, Dec. 2009.

[68] M. J. Wainwright, "Sharp thresholds for high-dimensional and noisy sparsity recovery using ℓ_1-constrained quadratic programming (lasso)," *IEEE Trans. Inf. Theory*, vol. 55, no. 5, pp. 2183–2202, May 2009.

[69] W. Wang, M. J. Wainwright, and K. Ramchandran, "Information-theoretic limits on sparse signal recovery: Dense versus sparse measurement matrices," *IEEE Trans. Inf. Theory*, vol. 56, no. 6, pp. 2967–2979, Jun. 2010.

[70] T. Zhang, "On the consistency of feature selection using greedy least squares regression," *J. Mach. Learn. Res.*, vol. 10, pp. 555–568, 2009.

[71] T. Zhang, "Adaptive forward-backward greedy algorithm for learning sparse representations," *IEEE Trans. Inf. Theory*, vol. 57, no. 7, pp. 4689–4708, Jul. 2011.

[72] P. Zhao and B. Yu, "On model selection consistency of lasso," *J. Mach. Learn. Res.*, no. 7, pp. 2541–2567, 2006.

Antony Joseph (S'10) received his Bachelor's and Master's degrees in Statistics from the Indian Statistical Institute in 2004 and 2006 respectively, and an M.A. degree in Statistics from Yale University in 2010. He is currently working towards his Ph.D. in Statistics (expected May, 2012), also from Yale, under the supervision of Prof. Andrew Barron.

Apart from Information Theory, his other interests include applied as well theoretical aspects of Statistics, with particular attention to problems in Statistical Learning.

Andrew R Barron (S'84--M'85--SM'00) was born in Trenton, NJ, on September 28, 1959. He received the B.S. degree in electrical engineering and mathematical sciences from Rice University, Houston, TX, in 1981, and the

M.S. and Ph.D. degrees in electrical engineering from Stanford University, Stanford, CA, in 1982 and 1985, respectively.

From 1977 to 1982, he was a consultant and summer employee of Adaptronics, Inc., McLean, VA. From 1985 until 1992, he was a faculty member of the University of Illinois at Urbana-Champaign in the Department of Statistics and the Department of Electrical and Computer Engineering. He was a Visiting Research Scholar at the Berkeley Mathematical Sciences Research Institute in the Fall of 1991 and Barron Associates, Inc., Standardsville, VA, in the Spring of 1992.

In 1992, he joined Yale University, New Haven, CT, as a Professor of Statistics, where he has served as Chair of Statistics from 1999–2006. His research interests include the study of information-theoretic properties in the topics of probability limit theory, statistical inference, high-dimensional function estimation, neural networks, model selection, communication, universal data compression, prediction, and investment theory.

Dr. Barron received (jointly with Bertrand S. Clarke) the 1991 Browder J. Thompson Prize (best paper in all IEEE TRANSACTIONS in 1990 by authors age 30 or under) for the paper "Information-Theoretic Asymptotics of Bayes Methods." Dr. Barron was an Institute of Mathematical Statistics Medallion Award recipient in 2005. He served on the Board of Governors of the IEEE Information Theory Society from 1995 to 1999, and was Secretary of the Board of Governors during 1989–1990. He has served as an Associate Editor for the IEEE TRANSACTIONS ON INFORMATION THEORY from 1993 to 1995, and the Annals of Statistics for 1995–1997.