On the Iterative Decoding of High Rate LDPC Codes With Applications in Compressed Sensing

Fan Zhang and Henry D. Pfister
Department of Electrical and Computer Engineering, Texas A&M University
{fanzhang,hpfister}@tamu.edu

***Abstract*—This paper considers the performance of (j,k)-regular low-density parity-check (LDPC) codes with message-passing (MP) decoding algorithms in the high rate regime. From a coding perspective, this analysis is interesting for a variety of channels including the binary erasure channel (BEC) and the q-ary symmetric channel (q-SC). The first result is that, for the BEC, the density evolution (DE) threshold scales as $\Theta(k^{-1})$ and the critical stopping ratio scales as $\Theta(k^{-j/(j-2)})$.**

The analysis for the q-SC with verification decoding is also applicable to the compressed sensing (CS) of strictly-sparse signals. Of particular note is the performance of CS systems based on LDPC codes and MP decoding. The analysis based on DE/stopping set analysis is used to analyze the CS systems with randomized/uniform reconstruction. The results show that strictly sparse signals can be reconstructed with a constant oversampling ratio when the number of measurements scales linearly with the sparsity of the signal.

I. Introduction

Compressed sensing (CS) is a relatively new area of signal processing that has recently received a large amount of attention. The basic idea is that many real-world signals (e.g., those sparse in some transform domain) can be reconstructed from a relatively small number of linear dot-product measurements. Its roots lie in the areas of statistics and signal processing [3], [8], [1], but it is also very much related to previous work in computer science [10] and applied mathematics [4], [11], [12]. CS is also very closely related to error correcting codes, and can be seen as source coding using linear codes over real numbers [21], [28], [29], [22], [6].

In this paper, we analyze the performance of low-density parity-check (LDPC) codes with verification decoding [13] as applied to CS. The resulting decoding algorithm is almost identical to that of Sudocodes [21], but a more suitable code ensemble is chosen and a more precise analysis is presented. Since most of the interesting applications of CS require very sparse (or compressible) signals, the natural mapping to coding implies very high rate codes. One new characteristic of this analysis, which is also interesting from a coding perspective, is that the performance estimates hold uniformly as the code rate approaches one. This allows us to explore the sparsity (or rate) regime that makes sense for compressed sensing.

This material is based upon work supported by the National Science Foundation under Grant No. 0747470.

An important implication of this work is that our randomized reconstruction system allows linear-time reconstruction of strictly-sparse signals with a constant oversampling ratio. In contrast, all previous reconstruction methods with moderate reconstruction complexity have an oversampling ratio which grows logarithmically with the signal dimension.

A. Background on LDPC Codes

LDPC codes are linear codes introduced by Gallager in 1962 [9] and re-discovered by Mackay in 1995 [16]. Binary LDPC codes are now known to be capacity approaching on various channels when the block length tends to infinity. They can be represented by a Tanner graph, where the i-th variable node is connected to the j-th check node if the entry on the i-th column and j-th row of its parity-check matrix is non-zero.

LDPC codes can be decoded by an iterative *message-passing* (MP) algorithm which passes messages between the variable nodes and check nodes iteratively. If the messages passed along the edges are probabilities, then the algorithm is also called *belief propagation* (BP) decoding. The performance of the MP algorithm can be evaluated using density evolution (DE) [19] and stopping set analysis [5] [18]. Both methods provide decoding thresholds for code ensembles.

B. Connections Between Coding and CS

1) Encoding and Decoding: The sparse graph representation of LDPC codes allows encoding and decoding algorithms to be implemented with linear complexity in the code length n. Since LDPC codes are usually defined over the finite field $GF(q)$ instead of the real numbers, we need to modify the encoding/decoding algorithm to deal with signals over real numbers. Each entry in the parity-check matrix is either 0 or a real number drawn from a continuous distribution. The parity-check matrix $\Phi \in \mathbb{R}^{m\times n}$ will be full-rank with high probability (w.h.p.) and is used as the measurement matrix in the CS system (e.g., the signal vector $x \in \mathbb{R}^n$ is observed as $y = \Phi x$).

The process of generating the observation symbols can also be seen in bipartite Tanner graph representation. Each non-zero entry in Φ is the edge-weight of its corresponding edge in this graph. Therefore, the observation process associated with a degree d check node is as follows:

1) Encoding: The observation symbol is the weighted (by the weights of the edges) sum of the d neighboring

signal components.

In this work, we only consider strictly sparse signals and we use two decoders based on verification which were proposed and analyzed in [13]. The second algorithm was also proposed independently for CS in [21]. The decoding process uses the following rules:

1) If a measurement is zero, then all the neighboring variable nodes are verified as zero.
2) If a check node is of degree one, verify the variable node with the value of the measurement.
3) [Enhanced verification] If two check nodes overlap in a single variable node and have the same measurement value, then verify that variable node to the value of the measurement.
4) Remove all verified variable nodes and the edges attached to them by subtracting out the verified values from the measurements.
5) Repeat steps 1-4 until decoding succeeds or makes no more progress.

Note the first algorithm follows steps 1, 2, 4 and 5. The second algorithm follows steps from 1 to 5. These two algorithms correspond to the first and second algorithms in [13] and are referred to as LM1 and LM2 in this paper. Note that LDPC codes with LM2 decoding is identical to the Sudocodes introduced in [21].

In general, the scheme described above does not guarantee that all verified symbols are actually correct. The event that a symbol is verified but incorrect is called false verification (FV). In order to guarantee there is no FV, one might add a constraint on the signal such that the weighted sum, of any subset of the non-zero neighbors of a check node, does not equal to zero. Another approach is to consider random signals with continuous distributions so that FV occurs with probability zero.

Verification decoding was originally introduced and analyzed for the q-SC. It is based on the observation that, over large alphabets, the probability that "two independent random numbers are equal" is quite small. This leads to the *verification assumption* that any two matching values (during decoding) are generated by the same set of non-zero coefficients. The primary connection between CS, codes over real numbers, and verification decoding lies in the fact that:

The verification assumption applies equally well to both large discrete alphabets and the real numbers.

2) Analysis Tools: Based on the bipartite graph structure, LDPC codes can be decoded efficiently using iterative MP algorithms. The average performance of MP decoding algorithms can be analyzed with density evolution (DE) [19] or extrinsic information transfer (EXIT) charts [25]. The concentration theorem [19] shows that random realizations of decoding are close to the average behavior w.h.p. as the block length goes to infinity. DE analysis provides a threshold below which decoding (or reconstruction) succeeds w.h.p.. The decoding threshold can be improved by optimizing the edge degree distribution (d.d.) pair $\lambda(x)$ and $\rho(x)$.

Decoding can also be analyzed using combinatorial methods such as stopping set analysis [5] and [18]. Stopping set analysis gives a threshold below which *all* error patterns can be recovered with certainty under the assumption of no FV. Note that DE and stopping set analysis lead to different thresholds in general. Since stopping set analysis implies uniform recovery of all the error patterns, instead of just most of them, the threshold given by stopping set analysis is always lower than the one given by DE. For example, for $(3, 6)$ regular codes over the BEC, the DE analysis shows most erasure patterns with size less than 43% of the code length can be corrected w.h.p. [14], but the result from stopping set analysis guarantees that most codes correct all erasure patterns with size less than 1.8% of the code length when $n \to \infty$.

Likewise, in CS systems, there are two standard measures of reconstruction: *uniform* reconstruction and *randomized* (or *non-uniform*) reconstruction. A CS system achieves randomized reconstruction if *most* randomly chosen measurement matrices recover *most* of the signals in the signal set. While a CS system achieves uniform reconstruction if there is a measurement matrix such that the decoder recovers *all* the signals in the signal set with certainty. Another criterion, which is between uniform reconstruction and randomized reconstruction, is what we call *uniform-in-probability* reconstruction. A CS system achieves uniform-in-probability reconstruction if, for any signal in the signal set, *most* randomly chosen measurement matrices realize successful decoding.

Since DE and the concentration theorem lead to w.h.p. statements for MP decoding over all signals and graphs, it is natural to adopt a DE analysis to evaluate the performance of randomized reconstruction CS systems based on LDPC codes. For uniform reconstruction, a stopping set analysis of the MP decoder is the natural choice. While this works for the BEC, the possibility of FV prevents this type of strong statement for verification decoding. If the non-zero entries of Φ are chosen randomly from a continuous distribution, however, then the probability of FV is zero for all signals. Therefore, one can use stopping set analysis to show that MP decoding of LDPC codes achieves uniform-in-probability reconstruction. The reader is cautioned that these results are somewhat brittle, however, because they rely on exact calculation and measurement of real numbers.

Understanding CS systems requires one to consider how the system parameters (e.g., the number of measurements and the sparsity of the signal) scale in the regime where the signal is both high-dimensional and extremely sparse. To compare results, we focus on *oversampling ratio* (i.e., the number of measurements divided by the number of non-zero elements in the signal) required for reconstruction. This leads us to a scaling law approach to the standard DE and stopping set analysis.

3) Decoding Algorithms: In CS, optimal decoding (in terms of oversampling ratio) requires a combinatorial search that is known to be NP-Hard [2]. Practical reconstruction algorithms tend to either be based on linear programming (e.g., basis pursuit (BP) [3]) or low-complexity iterative algorithms (e.g., Orthogonal Matching Pursuit (OMP) [26]). A wide range of algorithms allow one to trade-off the oversampling

ratio for reconstruction complexity. In [21], LDPC codes are used in the CS system and the algorithm is essentially identical to the verification based decoding proposed in [13]. The scaling law analysis shows the oversampling ratio for LDPC codes based CS system can be quite good. Encoding/decoding complexity is also a consideration. LDPC codes have sparse bipartite graph representation so that encoding and decoding algorithms with complexity linearly with the code length can be developed.

There are several existing MP decoding algorithms for LDPC codes over non-binary fields. In [14] and [24], analysis is introduced to find provably capacity-achieving codes for erasure channels under MP decoding. Metzner presents a modified majority-logic decoder in [17] that is similar to verification decoding. Davey and Mackay develop and analyze a symbol-level MP decoder over small finite fields [7]. Two verification decoding algorithms for large discrete alphabets are proposed by Luby and Mitzenmacher in [13] and called as LM1 and LM2 in this paper. The first and second capacity-achieving algorithms are presented by Shokrollahi and Wang in [23] and denoted as SW1 and SW2. The LMP algorithm [30] provides trade-offs between performance and complexity for SW1 and SW2. These algorithms are summarized in [30].

Since the scaling law analysis becomes quite difficult when complicated algorithms are applied, we consider only the (j,k)-regular code ensemble and the relatively simple algorithms LM1 and LM2. The rather suprising result is that even with regular codes and simple decoding algorithms, the scaling law implies that LDPC codes and MP decoding performs very well in CS systems with strictly-sparse vectors,

4) Signal Model: There are some significant differences between coding theory and CS. One of them is the signal model. The first difference is that coding theory typically uses discrete alphabets (see [27] for an exception to this) while CS deals with signals over the real numbers. Fortunately, some codes designed for large discrete alphabets (e.g., the q-ary symmetric channel) can be adapted to the real numbers. By exploring the connection and the analogy between real field and finite field with large q, the CS system can be seen as an essentially a syndrome-based source coding system [29]. Using the parity-check matrix of a non-binary LDPC code as the measurement matrix, the MP decoding algorithm can be used as the reconstruction algorithm.

The second difference in the signal model is that CS usually models the sparse signal $x \in \mathbb{R}^N$ as a random vector in an N-dimensional ℓ_r ball which is denoted as $U(\ell_r^N)$. The additional constraint $x \in U(\ell_r^N)$, which implies $(\sum_i |x_i|^r) \leq M^r$, defines an approximate sparsity property of the signal. As r approaches to zero, the decreasing reorder of the coefficients of x decays faster, i.e., $x_i^* \leq Mi^{-\frac{1}{r}}$ where the smallest M is the ℓ_r^N "norm" of x. In the extreme case, as $r \to 0$, the signal lives in an ℓ_0^N ball. This provides a partial ordering of the set $\{x | x \in U(\ell_0^N)\}$ and means that an x with a smaller ℓ_0^N "norm" is somehow preferred. This explains why ℓ_0^N minimization is a good recovery scheme for strictly sparse signals (e.g., signals in an ℓ_0^N ball). More generally, if the sparse signal lives in an ℓ_r^N ball, then minimizing the ℓ_r^N norm should give a good solution.

In information theory and coding theory, the most commonly used signal model is a probabilistic model, i.e., the signal is treated as a random variable and the pdf is used to describe the signal. The sparsity of the signal can be well described in the probabilistic model. For example, we can use a weighted sum of a unit impulse at zero and a uniform distribution to describe a strictly sparse signal. It can be shown that recovery in the probabilistic model is very similar to the recovery in deterministic model as long as the signal coefficients have the same marginal distributions by comparing the entropy of the signals in these two models.

5) Interesting Rate Regime: In coding theory, the code rate depends on the application and the interesting rate regime varies from close to zero to almost one. In CS systems, the signal is sparse in some domain and becomes increasingly sparse as the dimension increases. Intuitively, this means we can use codes with very little redundancy or very high code rate to represent the signal. So the interesting rate regime for CS systems is the high rate regime. We consider the relationship between the system parameters and how they scale as the rate goes to one. The answer lies in the scaling law analysis developed in this paper.

C. Structure of the Paper

In section II, we summarize the main results. In section III and section IV, we provide details and proofs for the main results. Some conclusions are given in section V.

II. Main Results

The main results of this paper are listed as follows. The details follow in section III and section IV. Note that all results hold for randomly-chosen regular LDPC codes with variable degree j and check degree k. For given variable degree j, we increase check degree k and see how the decoding threshold scales with j and k. The nice result is that the scaling law gives both conditions for successful reconstruction and a converse. Another interesting point is that randomized reconstruction is achieved, for CS of strictly-sparse signals, when the number of measurements scales linearly with the sparsity of the signal.

(i) [DE-BEC] For the BEC, there is a $K < \infty$ such that: a check-regular LDPC codes with average bit degree $j \geq 2$ and check-degree k can recover a $\delta < \bar{\alpha}_j j/(k-1)$ fraction of erasures (w.h.p. as $n \to \infty$) when $k \geq K$. The constant $\bar{\alpha}_j$ (independent of k) is essentially the fraction of the optimal $\delta^* = j/k$ achieved as the rate goes to one. Conversely, if the erasure probability $\delta > \bar{\alpha}_j j/(k-1)$, then decoding fails (w.h.p. as $n \to \infty$) for all k.

(ii) [SS-BEC] For any $\theta < 1$, there is a $K < \infty$ such that: for all $k \geq K$, a (j,k)-regular LDPC code with $j \geq 3$ can recover all erasures (w.h.p. as $n \to \infty$) of size $\theta ne\,(k-1)^{-j/(j-2)}$.

(iii) [DE-q-SC-LM1] For the q-SC, when one chooses a code randomly from the (j,k) regular ensemble with $j \geq 2$ and uses LM1 as decoding algorithm, then there is a $K_1 < \infty$ such that one can recover almost all error patterns of size $n\delta$ for $\delta < \bar{\alpha}_j (k-1)^{-j/(j-1)}$ (w.h.p. as $n \to \infty$) for all $k \geq K_1$.

Conversely, when $\delta > \bar{\alpha}_j (k-1)^{-j/(j-1)}$, there is a $K_2 < \infty$ such that the decoder fails (w.h.p. as $n \to \infty$) for all $k \geq K_2$.

(iv) [DE-q-SC-LM2] For the q-SC, when one chooses a code randomly from the (j,k) regular ensemble with $j \geq 3$ and uses LM2 as decoding algorithm, then there is a $K_1 < \infty$ such that one can recover almost all error patterns of size $n\delta$ for $\delta < \bar{\alpha}_j j/k$ (w.h.p. as $n \to \infty$). The constant $\bar{\alpha}_j$ (independent of k) is essentially the fraction of the optimal $\delta^* = j/k$ achieved as the rate goes to one. Conversely, there is a $K_2 < \infty$ such that the decoder fails (w.h.p. as $n \to \infty$) when $\delta > \bar{\alpha}_j j/k$ for all $k \geq K_2$.

(v) [SS-q-SC-LM1] For any $\theta < 1$, there is a $K < \infty$ such that: For all $k \geq K$, a (j,k)-regular LDPC code with $j \geq 3$ using LM1 decoding can recover (w.h.p as $n \to \infty$) all q-SC error patterns of size $\theta ne(k-1)^{-j/(j-2)}$ if no false verifications occur.

Note that the constants K, K_1, K_2 and $\bar{\alpha}_j$ in (i), (ii), (iii), (iv) and (v) are different, but for the simplicity of expression, we use the same notation without confusion.

III. High Rate Scaling Density Evolution

A. DE Scaling Law Analysis for the BEC

DE analysis provides an explicit recursion which connects the distributions of messages passed from variable nodes to check nodes at two consecutive iterations of MP algorithms. In the case of BEC, this task has been accomplished in [15] and [14]. It has been shown that the expected fraction of erasure messages which are passed in the i-th iteration, called x_i, evolves as $x_i = \delta\lambda(1-\rho(1-x_{i-1}))$ where δ is the erasure probability of the channel. For general channels, the recursion may be much more complicated because one has to track the general distributions which cannot be represented by a single parameter [20].

To illustrate the scaling law, we start by analyzing the BEC case. Although this is not applicable to CS, it motivates the scaling law analysis for the q-SC which is related to CS. Based on the DE analysis for the BEC, we will develop scaling laws which are much easier than the q-SC case. Many results will make use of the following simple lemma.

Lemma 1: For all $s \geq 0$ and $k^{1+s} > |x|$, the sequence $a_k = \left(1 - \frac{x}{k^{1+s}}\right)^k$ is strictly increasing in k and

$$1 - xk^{-s} \leq a_k \leq e^{-xk^{-s}}. \tag{1}$$

Proof: We restrict our attention to $x \geq 0$ because the proof is simplified in this case and the continuation does not require $x < 0$. We show that a_k is strictly increasing with k by considering the power series expansion of $\ln a_k$, which converges if $k^{1+s} > |x|$. This gives

$$\ln a_k = k \ln\left(1 - \frac{x}{k^{1+s}}\right) = -xk^{-s} - \sum_{i=2}^{\infty} \frac{x^i}{i\, k^{(1+s)i-1}}, \tag{2}$$

and keeping only the first term shows that $\ln a_k \leq -xk^{-s}$. Since all the terms are negative and decreasing with k, we see that a_k is strictly increasing with k. Since a_k is convex in x for $k^{1+s} > |x|$, the lower bound $a_k \geq 1 - xk^{-s}$ follows from tangent lower bound at $x = 0$. ∎

The scaling law of LDPC codes of check-regular ensemble over the BEC is shown by the following theorem.

Theorem 1: Consider a sequence of check-regular LDPC codes with fixed bit degree distribution $\lambda(x)$ and increasing check degree k. Let $j = \left(\int_0^1 \lambda(x)dx\right)^{-1}$ be the average bit degree and $\overline{\alpha}_j$, which is called α-threshold, be the largest α such that $\lambda\left(1 - e^{-\alpha j x}\right) \leq x$ for $x \in (0,1]$. For the erasure probability $\delta = \alpha j/(k-1)$, the iterative decoding of a randomly chosen length-n code from this ensemble fails (w.h.p as $n \to \infty$) for all k if $\alpha > \overline{\alpha}_j$. Conversely, if $\alpha < \overline{\alpha}_j$, then there exists a $K < \infty$ such that iterative decoding succeeds (w.h.p as $n \to \infty$) for all $k \geq K$.

Proof: Using the change of variable, $x_i = \frac{\overline{\alpha}_j j}{k-1} y_i$, the DE recursion can be scaled to get

$$y_{i+1} = f_k(y_i) \triangleq \frac{\alpha}{\overline{\alpha}_j} \lambda\left(1 - \left(1 - \frac{\overline{\alpha}_j j y_i}{k-1}\right)^{k-1}\right). \tag{3}$$

By Lemma 1, $(1 - \frac{x}{k-1})^{k-1}$ increases monotonically (for $x \leq k-1$) to e^{-x}, and we see that $f_k(y)$ decreases monotonically to $f_*(y) = \frac{\alpha}{\overline{\alpha}_j}\lambda\left(1 - e^{-\overline{\alpha}_j j y}\right)$. If $\alpha > \overline{\alpha}_j$, then (by the definition of $\overline{\alpha}_j$) $f_*(y) > y$ for some $y \in (0,1]$. Since $f_k(y) \geq f_*(y)$, the recursion $y_{i+1} = f_k(y_i)$ will not converge to zero (from $y_0 = 1$) and iterative decoding will fail for all k w.h.p. as $n \to \infty$.

If $\alpha < \overline{\alpha}_j$, then $f_*(y) < y$ for $y \in (0,1]$. Since $f_k(y) \searrow f_*(y)$, we can choose $K < \infty$ to be the first k such that $f_k(y) < y$ for $y \in (0,1]$. In this case, the recursion $y_{i+1} = f_k(y_i)$ will converge to zero (from $y_0 = 1$) for all $k \geq K$ and iterative decoding will succeed w.h.p. as $n \to \infty$. ∎

Proposition 1: For (j,k) regular LDPC codes, the α-threshold is given by $\overline{\alpha}_j$ with $\overline{\alpha}_2 = 0.5$, $\overline{\alpha}_3 \approx 0.8184$, and $\overline{\alpha}_4 \approx 0.7722$.

Proof: See [31]. ∎

Remark 1: For example, consider $j=3$ with $\overline{\alpha}_3 = 0.8184$. If $\alpha = 0.75$, then numerical results show that $K = 9$ suffices and DE converges for all $k \geq 9$ when $\delta < 3(0.75)/(k-1)$. This implies that $(3,k)$-regular LDPC codes correct w.h.p. at least 75% of the the optimal $\delta^* = 3/k$ fraction of erasures for all $k \geq 9$.

The above theorem relies on the concentration theorem of [20]. This concentration theorem holds only when k is fixed as $n \to \infty$. If we would like to make a similar statement for $k = \Theta(n^\kappa)$, then it is not immediately clear how to proceed. Our approach is based on first removing all correctly received symbol nodes. This reduces the initial graph with n symbol nodes and very large degrees to a much smaller graph with roughly $\Theta(n^{1-\kappa})$ symbol nodes and a Poisson check distribution with finite mean. Applying the original concentration theorem to the reduced graph gives the result.

B. DE Scaling Law Analysis for the q-SC

1) DE Scaling Law Analysis for LM1: For the simplicity of our analysis, we only consider (j,k)-regular code ensemble and the LM1 decoding algorithm [13] for the q-SC with error probability δ. The DE recursion for LM1 is (from [13])

$$x_{i+1}=\delta\left(1-\left[1-(1-\delta)\left(1-(1-x_i)^{k-1}\right)^{j-1}-x_i\right]^{k-1}\right)^{j-1} \quad (4)$$

where x_i is the fraction of unverified messages in the i-th iteration. Our analysis of the scaling law relies on the following lemma.

Lemma 2: Let the functions $g_{k+1}(x)$ and $\overline{g}_{k+1}(x)$ be defined by

$$g_{k+1}(x) \triangleq \frac{\alpha}{\overline{\alpha}_j}\left(1-\left[1-\left(1-\frac{\alpha}{k^{j/(j-1)}}\right)\left(1-\left(1-\frac{\overline{\alpha}_j x}{k^{j/(j-1)}}\right)^k\right)^{j-1}-\frac{\overline{\alpha}_j x}{k^{j/(j-1)}}\right]^k\right)^{j-1}$$

$$\overline{g}_{k+1}(x) \triangleq \frac{\alpha}{\overline{\alpha}_j}\left(1-\left[1-\frac{\overline{\alpha}_j^{j-1}x^{j-1}}{k}-\frac{\overline{\alpha}_j x}{k^{j/(j-1)}}\right]^k\right)^{j-1},$$

where $\overline{\alpha}_j \geq 1$, $\alpha \in (0,\overline{\alpha}_j]$, and $j \geq 2$. For $x \in (0,1]$ and $k > \overline{\alpha}_j^{j-1}$, these functions satisfy (i) $g_k(x) \leq \overline{g}_k(x)$, (ii) $\overline{g}_k(x)$ is monotonically decreasing with k for $k > \overline{\alpha}_j^{j-1}$, and (iii) $\lim_{k\to\infty} g_k(x) = \lim_{k\to\infty} \overline{g}_k(x) = \frac{\alpha}{\overline{\alpha}_j}\left(1-e^{-\overline{\alpha}_j^{j-1}x^{j-1}}\right)^{j-1}$.

Proof: See [31]. ∎

Theorem 2: Consider a sequence of (j,k)-regular LDPC codes with fixed variable degree $j \geq 2$ and increasing check degree k. Let $\bar{\alpha}_j$ be the largest α such that $(1-e^{-\alpha^{j-1}x^{j-1}})^{j-1} \leq x$ for $x \in (0,1]$. If the sparsity of the signal is $n\delta$ for $\delta = \alpha(k-1)^{-j/(j-1)}$ and $\alpha < \bar{\alpha}_j$, then there exist a K_1 such that by randomly choosing a length-n code from the (j,k) regular LDPC code ensemble, LM1 reconstruction succeeds (w.h.p as $n\to\infty$) for all $k \geq K_1$. Conversely, if $\alpha > \bar{\alpha}_j$ then there exists a K_2 such that LM1 reconstruction fails (w.h.p as $n\to\infty$) for all $k \geq K_2$.

Proof: Scaling (4) using the change of variables $\delta = \alpha(k-1)^{-j/(j-1)}$ and $x_i = \overline{\alpha}_j y_i (k-1)^{-j/(j-1)}$ gives $y_{i+1} = g_k(y_i)$. The function $\overline{g}_k(x)$ also allows us to define the upper bound $z_{i+1} = \overline{g}_k(z_i)$ where $z_i \leq y_i$ implies $z_{i+1} \leq y_{i+1}$.

Since $\left(1-\frac{x}{k}\right)^k$ increases monotonically to e^{-x}, we see that $\overline{g}_k(y)$ decreases monotonically to $g_*(y)$. If $\alpha < \overline{\alpha}_j$, then $g_*(y) < y$ for all $y \in (0,1]$. Since $g_k(y) \leq \overline{g}_k(y) \searrow g_*(y)$, we can choose $K_1 < \infty$ to be the first k such that $\overline{g}_k(y) < y$ for all $y \in (0,1]$. In this case, the recursion $y_{i+1} = g_k(y_i)$ will converge to zero (from $y_0 = 1$) for all $k \geq K_1$ and iterative decoding will succeed w.h.p. as $n\to\infty$.

If $\alpha > \overline{\alpha}_j$, then (by the definition of $\overline{\alpha}_j$) $g_*(y) > y$ for some $y \in (0,1]$. Since $\lim_{k\to\infty} g_k(y) = g_*(y)$, there exists a K_2 such that, for all $k \geq K_2$, the recursion $y_{i+1} = g_k(y_i)$ will not converge to zero (from $y_0 = 1$) and iterative decoding will fail w.h.p. as $n\to\infty$. ∎

Remark 2: If a randomly chosen code from the (j,k) regular ensemble is applied to a CS system with LM1 reconstruction, then randomized reconstruction succeeds (w.h.p as $n\to\infty$) when the sparsity is $n\delta$ with $\delta < \bar{\alpha}_j(k-1)^{-j/(j-1)}$. This requires $m = \gamma(n\delta)$ measurements with an oversampling ratio of $\gamma > \gamma_0 = \bar{\alpha}_j^{-(j-1)/j}\delta^{-1/j} j$.

Proposition 2: The $\overline{\alpha}_j$ constant in Theorem 2 is given by $\bar{\alpha}_2 = 1$, $\bar{\alpha}_3 \approx 1.873$, $\bar{\alpha}_4 \approx 1.664$ and $\bar{\alpha}_5 \approx 1.520$. We also find that (i) $\bar{\alpha}_{j+1} \leq \bar{\alpha}_j$ for $j \geq 3$ and (ii) $\lim_{j\to\infty} \bar{\alpha}_j = 1$.

Proof: Recall that $\bar{\alpha}_j$ is defined as the largest α s.t. $\left(1-e^{-\alpha^{j-1}x^{j-1}}\right)^{j-1} \leq x$ for $x \in (0,1]$. So $\bar{\alpha}_j$ can be written as

$$\bar{\alpha}_j = \inf_{x\in(0,1]} h_j(x) \quad (5)$$

where $h_j(x) = \left(-\log\left(1-x^{1/(j-1)}\right)x^{(1-j)}\right)^{1/(j-1)}$. Notice that $h_j(x)$ is a monotonically increasing function of x when $j = 2$. So we have

$$\bar{\alpha}_2 = \lim_{x\to 0} h_j(x) = 1. \quad (6)$$

When $j \geq 3$, $h_j(x)$ goes to infinity when x goes to either 0 or 1, so the infimum is achieved at an interior point x_j^*. By setting derivative of x to zero, x_j^* is

$$x_j^* = \left(1+\left((j-1)^2 W_{-1}\left(-e^{-1/(j-1)^2}/(j-1)^2\right)\right)^{-1}\right)^2. \quad (7)$$

By solving this numerically, we find that $x_3^* \approx 0.816$, $x_4^* \approx 0.939$ and $x_5^* \approx 0.971$. Substituting x_j^* into Eq. (5), we have $\bar{\alpha}_3 \approx 1.873$, $\bar{\alpha}_4 \approx 1.664$ and $\bar{\alpha}_5 \approx 1.520$. ∎

Corollary 1: For regular LDPC codes and LM1 reconstruction, choosing $j = \lceil \ln\frac{1}{\delta} \rceil$ gives a uniform lower bound on the oversampling ratio (as $\delta \to 0$) of $\lceil \ln\frac{1}{\delta} \rceil e$.

Proof: The minimum oversampling ratio is $\gamma_0 = \bar{\alpha}_j^{-(j-1)/j} j\delta^{-1/j} \leq j\delta^{-1/j}$ and we choose $j = \lceil \ln\frac{1}{\delta} \rceil$. Taking the logarithm of both sides shows that

$$\ln\gamma_0 \leq \ln\left\lceil \ln\frac{1}{\delta}\right\rceil + \frac{1}{\lceil \ln\frac{1}{\delta}\rceil}\ln\frac{1}{\delta} \leq \ln\left\lceil \ln\frac{1}{\delta}\right\rceil + 1. \quad (8)$$

∎

2) Scaling Law Analysis Based on DE for LM2: For the second algorithm in [13], the DE recursion for the fraction x_i of unverified messages in the i-th iteration is

$$x_{i+1} = \delta\Big(\lambda\left(1-\rho\left(1-x_i\right)\right) + \lambda'\left(1-\rho\left(1-x_i\right)\right) \left(\rho\left(1-x_i\right) - \rho\left(1-(1-\delta)\lambda\left(1-\rho\left(1-x_i\right)\right)-x_i\right)\right)\Big). \quad (9)$$

Like the analysis of LM1, we first introduce a lemma to bound the scaled DE equation.

Lemma 3: The functions $g_k(x)$ and $\bar{g}_k(x)$ are defined as

$$g_k(x) \triangleq \frac{\alpha}{\bar{\alpha}_j}\left((s(x))^{j-1} + (j-1)(s(x))^{j-2}\left(\left(1-\frac{\alpha j x}{k}\right)^{k-1} - \left(1-\frac{\alpha j x}{k}-\left(1-\frac{\alpha j}{k}\right)(s(x))^{j-1}\right)^{k-1}\right)\right),$$

where $s(x) = 1-\left(1-\frac{\alpha j x}{k}\right)^{k-1}$ and

$$\bar{g}_k(x) \triangleq \frac{\alpha}{\bar{\alpha}_j}\left(1-\left(1-\frac{\alpha j x}{k}\right)^k\right)^{j-1} + (j-1)\left(1-\left(1-\frac{\alpha j x}{k}\right)^k\right)^{j-2}\left(1-\frac{\alpha j x}{k}\right)^k.$$

For $x \in (0,1]$ and $k > \alpha$, these functions satisfy (i) $\bar{g}_k(x) > g_k(x)$, (ii) $\lim_{k\to\infty} g_k(x) = \lim_{k\to\infty} \overline{g}_k(x) = g_*(x)$ where

$$g_*(x) \triangleq \frac{\alpha e^{\alpha j x}\left(1-e^{-\alpha j x}\right)^j\left(e^{\alpha j x}+j-2\right)}{\bar{\alpha}_j\left(e^{\alpha j x}-1\right)^2}, \qquad (10)$$

and (iii) $\bar{g}_k(x)$ is a monotonically decreasing function of k.

Proof: See [31]. ∎

Theorem 3: Consider a sequence of (j,k)-regular LDPC codes with variable node degree $j \geq 3$. Let $\overline{\alpha}_j$ be the largest α such that $(e^{\alpha j x}-1)^{-2}e^{\alpha j x}(1-e^{-\alpha j x})^j(e^{\alpha j x}+j-2) \leq x$ for $x \in (0,1]$. If the sparsity of the signal is $n\delta$ with $\delta = n\alpha j/k$ and $\alpha < \overline{\alpha}_j$, then there exists a K_1 such that LM2 reconstruction succeeds (w.h.p as $n \to \infty$) for all $k \geq K_1$. Conversely, if $\alpha > \overline{\alpha}_j$ then there exists a K_2 such that LM2 decoding fails (w.h.p as $n \to \infty$) for all $k \geq K_2$.

Proof: The LM2 DE recursion is given by (9). Using the change of variables $x_i = \frac{\overline{\alpha}_j j}{k} y_i$ and $\delta = \frac{\alpha j}{k}$, the scaled DE equation can be written as $y_{i+1} = g_k(y_i)$. Taking the limit as $k \to \infty$ gives $y_{i+1} = g_*(y_i)$.

If $\alpha < \overline{\alpha}_j$, then the definition of $\bar{\alpha}_j$ implies that $g_*(y) < y$ for $y \in (0,1]$. Since $g_k(y) \leq \overline{g}_k(y) \searrow g_*(y)$ (by Lemma 3), we can choose $K_1 < \infty$ to be the first k such that $\overline{g}_k(y) < y$ for $y \in (0,1]$. In this case, the recursion $y_{i+1} = g_k(y_i)$ will converge to zero (from $y_0 = 1$) for all $k \geq K_1$ and iterative decoding will succeed w.h.p. as $n \to \infty$.

If $\alpha > \overline{\alpha}_j$, then (by the definition of $\overline{\alpha}_j$) $g_*(y) > y$ for some $y \in (0,1]$. In this case, there is a K_2 and y such that $g_k(y) > y$ for all $k \geq K_2$, and the recursion $y_{i+1} = g_k(y_i)$ does not converge to zero (from $y_0 = 1$) and iterative decoding will fail w.h.p. as $n \to \infty$.

For $j = 2$, the quantity $\overline{\alpha}_2$ is undefined because $(e^{\alpha j x} - 1)^{-2}e^{\alpha j x}(1-e^{-\alpha j x})^j(e^{\alpha j x}+j-2) = 1$. This implies that $(2,\ k)$ regular LDPC codes with the LM2 decoding algorithm do not satisfy obey this scaling law. ∎

Remark 3: If a randomly chosen code from the (j,k) regular ensemble is applied to a CS system with LM2 reconstruction, then randomized reconstruction succeeds (w.h.p as $n \to \infty$) when the sparsity is $n\delta$ with $\delta < \bar{\alpha}_j j/k$. This requires $m \geq \gamma(n\delta)$ measurements and an oversampling ratio of $\gamma > \gamma_0 = 1/\bar{\alpha}_j$.

Remark 4: For (j,k) regular LDPC codes, the α-threshold of LM2 is given by $\overline{\alpha}_j$ and can be calculated numerically to get $\overline{\alpha}_3 = \frac{1}{6}$, $\overline{\alpha}_4 \approx 0.34$ and $\overline{\alpha}_5 \approx 0.37$.
The interesting part of this result is that the number of measurements needed for randomized reconstruction with LM2 scales linearly with the sparsity of the signal. All previous reconstruction methods with reasonable complexity require a super-linear number of measurements.

Note that the proof of concentration theorem in [20] also does not apply for LM2 when k grows with n. By extending the idea used in the BEC case, we can show that a concentration theorem holds in this case as well.

IV. Scaling Laws Based on Stopping Set Analysis

DE analysis provides the threshold below which the *randomized* (or *non-uniform*) recovery is guaranteed, in the following sense: the measurement matrix is chosen from some distribution, and the reconstruction is guaranteed to be correct for a given signal w.h.p.. If the reconstruction is guaranteed for all signals, it is called *uniform* recovery. If the probability only lies in the matrix, the construction is called uniform-in-probability recovery. According to the analysis in section III, we know that the number of measurements needed for randomized recovery by using LM2 scales linearly with the sparsity of the signal. Note that the probability of imperfect recovery lies in both the signal and the measurement matrix.

In this section, we will analyze the performance of the MP algorithm with uniform-in-probability recovery in the high rate regime. This can be done by the stopping set analysis of the code structure in coding theory similar to [18] because stopping set is the signal pattern decoding algorithm can not proceed and declares decoding failure.

A stopping set is defined as a set of nodes such that the decoding algorithm stops making progress. Following the definition in [18], Let $G = (V \cup C, E)$ be the Tanner graph of a code where V is the set of variable nodes, C is the set of check nodes and E is the set of edges between V and C. We define a subset U of V as a BEC stopping set if no check node is connected to U via a single edge.

A. Scaling Law Analysis for Stopping Sets on the BEC

The average stopping set distribution $E_{n,j,k}(s)$ is defined as the average (over the ensemble) number of stopping sets in a randomly chosen code (j,k) regular code with n variable nodes. The normalized stopping set distribution $\gamma_{j,k}(\alpha)$ is defined as $\gamma_{j,k}(\alpha) \triangleq \lim_{n\to\infty} \frac{1}{n} \log E_{n,j,k}(n\alpha)$. The critical stopping ratio $\alpha^*_{j,k}$ is defined as $\alpha^*_{j,k} \triangleq \inf\{\alpha > 0 : \gamma_{j,k}(\alpha) \geq 0\}$. Intuitively, when the normalized size of the stopping set is greater than or equal to $\alpha^*_{j,k}$, the average number of stopping sets grows exponentially with n. When the normalized size of the stopping set is less than $\alpha^*_{j,k}$, the average number of stopping sets decays exponentially with n. In fact, there exist codes with no stopping sets of normalized size less than $\alpha^*_{j,k}$. Therefore, the quantity $\alpha^*_{j,k}$ can also be thought of as a *deterministic decoding threshold.*

The normalized average stopping set distributions $\gamma_{j,k}(\alpha)$ for (j,k) regular ensembles with BEC is given by [18]

$$\gamma_{j,k}(\alpha) \leq \gamma_{j,k}(\alpha,x) = \frac{j}{k}\log\left(\frac{(1+x)^k - kx}{x^{k\alpha}}\right) - (j-1)h(\alpha)$$

where $h(\cdot)$ is the binary entropy function and the bound holds for any $x \geq 0$. The optimum value x_0 is the unique positive solution of $\frac{x((1+x)^{k-1}-1)}{(1+x)^k - kx} = \alpha$. This gives the following theorem.

Theorem 4: For any $\theta < 1$, there is a $K < \infty$ such that, for all $k \geq K$, a randomly chosen (j,k) regular LDPC code ($j \geq 3$) will (w.h.p. as $n \to \infty$) correct all erasure patterns of size less than $\theta ne(k-1)^{-j/(j-2)}$.

Sketch of Proof: Since there is no explicit solution for x_0, we assume $\alpha = o(\frac{1}{k})$, expand this expression around $x = 0$ and solve for x_0; this gives $x_0 \approx \sqrt{\frac{\alpha}{k-1}}$. Since $\gamma(\alpha) \leq \gamma(\alpha, x)$ holds for all $x \geq 0$, we have

$$\gamma(\alpha) \leq \frac{j}{k} \log \left(\frac{\left(1+\sqrt{\frac{\alpha}{k-1}}\right)^k - k\sqrt{\frac{\alpha}{k-1}}}{\frac{\alpha}{k-1}^{\frac{k\alpha}{2}}} \right) - (j-1)h(\alpha). \quad (11)$$

Next we expand the RHS of (11) around $\alpha = 0$ and neglect the high order terms; solving for α gives an upper bound on the critical stopping ratio

$$\alpha^*_{j,k} \leq \exp\left(\frac{j-2-j\log(k-1)}{j-2}\right).$$

It can be shown that this bound on $\alpha^*_{j,k}$ is tight as $k \to \infty$. This means that, for any $\theta < 1$, there is a K such that $\theta e(k-1)^{-j/(j-2)} \leq \alpha^*_{j,k} \leq e(k-1)^{-j/(j-2)}$ for all $k > K$. Therefore, the critical stopping ratio $\alpha^*_{j,k}$ scales like $e(k-1)^{-j/(j-2)}$ as $k \to \infty$. ∎

B. Stopping Set Analysis for the q-SC with LM1

A stopping set for LM1 is defined by considering a decoder where S, T, U are disjoint subsets of V corresponding to verified, correct, and incorrect variable nodes. Decoding progresses if and only if (i) a check node has all but one edge attached to S or (ii) a check node has all edges attached to $S \cup T$. Otherwise, the pattern is a stopping set. In the stopping set analysis for q-SC, we can define $E_{n,j,k}(\alpha, \beta)$ as the *average number of stopping sets* with $|T| = n\alpha$ correctly received variable nodes and $|U| = n\beta$ incorrectly received variable nodes where n is the code length. $E_{n,j,k}(\alpha, \beta)$ can be calculated as follows,

$$E_{n,j,k}(\alpha,\beta) = \frac{\binom{n}{n\alpha, n\beta, n(1-\alpha-\beta)} c_{n,k}(\alpha,\beta)}{\binom{nj}{nj\alpha, nj\beta, nj(1-\alpha-\beta)}}$$

where $c_{n,k}(\alpha, \beta) \triangleq$

$$\text{Coeff}\Big(\Big(1+(1+x+y)^k - ky - (1+x)^k\Big)^{n\frac{j}{k}}, x^{jn\alpha} y^{jn\beta}\Big).$$

We are interested in the growth rate of $E_{n,j,k}(\alpha, \beta)$. Particularly, we are interested in finding the critical size of the stopping sets above which the average number of stopping sets grows exponentially with n. In the asymptotic analysis, we are interested in the *normalized average stopping set distribution* $\gamma_{j,k}(\alpha, \beta)$ which is defined as

$$\gamma_{j,k}(\alpha,\beta) = \lim_{n\to\infty} \frac{1}{n} \log E_{n,j,k}(\alpha,\beta) \quad (12)$$

The *critical stopping ratio* $\beta^*_{j,k}$ is defined as

$$\beta^*_{j,k} = \inf\{\beta \in [0,1] : \sup_{\alpha \in [0,1-\beta]} \gamma_{j,k}(\alpha,\beta) \geq 0\}. \quad (13)$$

Notice that the average number of stopping sets with normalized size less than $\beta^*_{j,k}$ decays exponentially with n. There also exists a (j, k) regular LDPC code with no stopping sets of normalized size less than $\beta^*_{j,k}$. One might conclude that iterative decoding succeeds deterministically for this code (if the normalized number of errors is less than $\beta^*_{j,k}$), but the possibility of false verification during the decoding process prevents this.

Theorem 5: The normalized average stopping set distributions $\gamma_{j,k}(\alpha, \beta)$ for LM1 is

$$\begin{aligned}\gamma_{j,k}(\alpha,\beta) &\leq \gamma_{j,k}(\alpha,\beta;x_0,y_0) \\ &= \frac{j}{k}\log\frac{\left(1+(1+x_0+y_0)^k - ky_0 - (1+x_0)^k\right)}{x_0^{k\alpha} y_0^{k\beta}} \\ &\quad + (1-j)h(\beta,\alpha,1-\beta-\alpha) \quad (14)\end{aligned}$$

where (x_0, y_0) is the positive solution of

$$\frac{x\left((1+x+y)^{k-1} - (1+x)^{k-1}\right)}{1+(1+x+y)^k - ky - (1+x)^k} = \alpha \quad (15)$$

and

$$\frac{y\left((1+x+y)^{k-1} - 1\right)}{1+(1+x+y)^k - ky - (1+x)^k} = \beta. \quad (16)$$

Proof: Using Stirling's formula and a Chernoff-type bound for $c_{n,k}(\alpha, \beta)$, we have $\gamma_{j,k}(\alpha, \beta; x, y) \triangleq$

$$\lim_{n\to\infty}\frac{1}{n}\log\exp\Bigg(nh(\beta,\alpha,1-\beta-\alpha)+n(1-R)$$
$$\log\frac{1+(1+x+y)^k-ky-(1+x)^k}{x^{k\alpha}y^{k\beta}} - njh(\beta,\alpha,1-\beta-\alpha)\Bigg).$$

Optimizing the bound over x, y gives $\gamma_{j,k}(\alpha, \beta; x_0, y_0)$ where x_0, y_0 as the unique positive solution of (15) and (16). ∎

C. Scaling Law Analysis for LM1 Stopping Sets

In CS literature, we are only interested in the scenario that β is small. It means we need to perform stopping set analysis in the high rate regime or to the signal vectors with sparse support. For the convenience of analysis, we only derive the analysis for (j, k) regular codes and it can be generalized to irregular codes [18]. In our analysis, the the variable node degree j is fixed and the check node degree k is increasing. By calculating the scaling law of $\gamma_{j,k}(\alpha, \beta)$, we find the uniform-in-probability recovery decoding threshold $\beta^*_{j,k}$ which tells us the relationship between the minimum number of measurements needed for uniform-in-probability recovery and the sparsity of the signal.

For the scaling law analysis, we need to do Taylor expansion around $(x, y) = (0, 0)$ or $(\alpha, \beta) = (0, 0)$. We will first show the expansion converges under some assumptions.

Lemma 4: In (15) and (16), if $\beta = \Theta\left((k-1)^{-j/(j-2)}\right)$, either $\alpha = \Theta(\beta)$, $x = \Theta\left((k-1)^{-(j-1)/(j-2)}\right)$ and $y = \Theta\left((k-1)^{-(j-1)/(j-2)}\right)$ or $\alpha = o(\beta)$, $y = \Theta\left((k-1)^{-(j-1)/(j-2)}\right)$ and $x = o(y)$ is satisfied.

Proof: See [31]. ∎

Theorem 6: Consider an LDPC code on the q-SC using the LM1 decoding algorithm. For any $\theta < 1$, there is a $K < \infty$ such that, for all $k \geq K$, a randomly chosen (j, k) regular LDPC code corrects all error patterns (assuming no false verification) of size $\theta ne(k-1)^{-j/(j-2)}$.

Sketch of Proof: We derive the scaling law for the stopping set analysis equation (14) for the two possible cases: (i) $x = o(y)$ and (ii) $x = \Theta(y)$.

First, if $x = o(y)$, we do the Taylor expansion of (15) and (16) to have the approximation for x and y as

$$x \approx \alpha/\sqrt{\beta(k-1)} \text{ and } \; y \approx \sqrt{\beta}/\sqrt{k-1}. \qquad (17)$$

Note that in this case, the product of x and y still behaves like $\frac{\alpha}{k-1}$, but α decays faster than β, i.e., $\alpha = o(\beta)$. So, we perform a Taylor expansion of (14) around $x = 0$ and plug in the approximation of x and y into the logarithm function. Then, we substitute $\alpha = \beta^{1+\delta}$ and expand γ around $\beta = 0$ we get

$$\gamma_{j,k}(\alpha,\beta) = \frac{1}{2}\beta\left((j-2)\left((\log\beta)-1\right)+j\log(k-1)\right)+o(\beta). \qquad (18)$$

If we neglect the high order terms and set the RHS to zero, then we have

$$\beta^*_{j,k} = e^{\frac{j-2-j\log(k-1)}{j-2}} = e(k-1)^{-j/(j-2)}.$$

Taking into account a few more details shows that the $x = o(y)$ assumption implies that $\beta^*_{j,k} \sim e(k-1)^{-j/(j-2)}$ as $k \to \infty$.

Next, we deal with the case $x = \Theta(y)$. The expansion of (15) and (16) gives the approximation of x and y as follows,

$$x \approx \alpha/\sqrt{(\beta-\alpha)(k-1)} \text{ and } y \approx \sqrt{(\beta-\alpha)/(k-1)}. \qquad (19)$$

Analysis shows that this also leads to the scaling rate $(k-1)^{-j/(j-2}$ with a smaller constant. Since the bound $\gamma_{j,k}(\alpha,\beta;x,y)$ is valid for any choice of x, y, we are free to choose the larger constant given by the first bound.

One subtlety not addressed here is that stopping sets with size sublinear in n need to be considered separately. The full proof shows that there are no sublinear stopping sets [31]. ■

Remark 5: In a CS system with strictly sparse signals and LM1 reconstruction, we have uniform-in-probability reconstruction (w.h.p. as $n \to \infty$) of all signals with sparsity at most $n\delta$ where $\delta < e(k-1)^{-j/(j-2)}$. This requires $m = \gamma(n\delta)$ measurements and an oversampling rate of $\gamma > \gamma_0 = e^{-(j-2)/j} j\delta^{-2/j}$.

V. Conclusion

We analyze message-passing decoding algorithms for LDPC codes in the high rate regime. The results can be applied to compressed sensing systems with strictly-sparse signals. A high rate analysis based on DE is used to derive the scaling law for randomized reconstruction CS systems and stopping set analysis is used to analyze uniform-in-probability reconstruction. The scaling law analysis gives the surprising result that LDPC codes, together with LM2 algorithm, allow randomized reconstruction when the number of measurements scales linearly with the sparsity of the signal.

References

[1] E. J. Candès, J. Romberg, and T. Tao. Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information. *IEEE Trans. Inform. Theory*, 52(2):489–509, 2006.

[2] E. J. Candès and T. Tao. Decoding by linear programming. *IEEE Trans. Inform. Theory*, 51(12):4203–4215, 2005.

[3] S.S. Chen, D.L. Donoho, and M.A. Saunders. Atomic decomposition by basis pursuit. *SIAM J. Sci. Comp.*, 20(1):33–61, 1998.

[4] A. Cohen, W. Dahmen, and R. DeVore. Compressed sensing and best k-term approximation. *IGPM Report, RWTH-Aachen*, July 2006.

[5] C. D., D. Proietti, E. Telatar, T. J. Richardson, and R. Urbanke. Finite-length analysis of low-density parity-check codes on the binary erasure channel. *IEEE Trans. Inform. Theory*, 48(6):1570–1579, June 2002.

[6] Wei Dai and Olgica Milenkovic. Weighted superimposed codes and constrained integer compressed sensing. submitted to *IEEE Trans. on Inform. Theory* also available in Arxiv preprint cs.IT/0806.2682v1, 2008.

[7] M. Davey and D. MacKay. Low density parity check codes over GF(q). 2:58–60, 1998.

[8] D. L. Donoho. Compressed sensing. *IEEE Trans. Inform. Theory*, 52(4):1289–1306, 2006.

[9] R. G. Gallager. Low-density parity-check codes. *IEEE Trans. Inform. Theory*, 8(1):21–28, January 1962.

[10] A. C. Gilbert, M. J. Strauss, J. A. Tropp, and R. Vershynin. One sketch for all: Fast algorithms for compressed sensing. In *in Proceedings of the ACM Symposium on the Theory of Computing (STOC 2007)*, 2007.

[11] E. D. Gluskin. On some finite-dimensional problems in the theory of widths. *Vestnik Leningrad Univ. Math*, 14:163-170, 1982.

[12] W. Johnson and J. Lindenstrauss. Extensions of lipschitz maps into hilbert space. *Contemp. Math.*, 26:189–206, 1984.

[13] M. Luby and M. Mitzenmacher. Verification-based decoding for packet-based low-density parity-check codes. *IEEE Trans. Inform. Theory*, 51(1):120–127, 2005.

[14] M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi, and D. A. Spielman. Efficient erasure correcting codes. *IEEE Trans. Inform. Theory*, 47(2):569–584, February 2001.

[15] M. G. Luby, M. Mitzenmacher, and M. Amin Shokrollahi. Practical loss-resilient codes. In *Proc. 29th Annu. ACM Symp. Theory of Computing*, pages 150–159, 1997.

[16] D. J. C. MacKay. Good error-correcting codes based on very sparse matrices. *IEEE Trans. Inform. Theory*, 45(2):399–431, March 1999.

[17] J. J. Metzner. Majority-logic-like decoding of vector symbols. 44:1227–1230, October 1996.

[18] A. Orlitsky, K. Viswanathan, and J. Zhang. Stopping set distribution of LDPC code ensembles. *IEEE Trans. Inform. Theory*, 51(3):929–953, 2005.

[19] T. Richardson, M. A. Shokrollahi, and R. Urbanke. Design of capacity-approaching irregular low-density parity-check codes. *IEEE Trans. Inform. Theory*, 47:619–637, February 2000.

[20] T. Richardson and R. Urbanke. The capacity of low-density parity-check codes under message-passing decoding. *IEEE Trans. Inform. Theory*, 47:599–618, February 2001.

[21] S. Sarvotham, D. Baron, and R. G. Baraniuk. Sudocodes–fast measurement and reconstruction of sparse signals. In *Proc. IEEE Int. Symp. Information Theory*, pages 2804–2808, Seattle, WA, July 2006.

[22] S. Sarvotham, D. Baron, and R.G. Baraniuk. Compressed sensing reconstruction via belief propagation. Technical Report ECE-06-01, Rice University, July 2006.

[23] A. M. Shokrollahi and W. Wang. Low-density parity-check codes with rates very close to the capacity of the q-ary symmetric channel for large q. Personal communication.

[24] M. A. Shokrollahi. New sequences of linear time erasure codes approaching the channel capacity. In *Applicable Algebra in Eng., Commun. Comp.*, pages 65–76, 1999.

[25] S. ten Brink. Convergence behavior of iteratively decoded parallel concatenated codes. *IEEE Trans. Inform. Theory*, 49:1727–1737, October 2001.

[26] J. A. Tropp and A. C. Gilbert. Signal recovery from random measurements via orthogonal matching pursuit. *IEEE Trans. Inform. Theory*, 53(12):4655–4666, 2007.

[27] J. K. Wolf. Redundancy, the discrete Fourier transform, and impulse noise cancellation. 31(3):458–461, March 1983.

[28] W. Xu and B. Hassibi. Efficient compressive sensing with deterministic guarantees using expander graphs. In *Proc. IEEE Inform. Theory Workshop*, pages 414–419, Lake Tahoe, CA, September 2007.

[29] F. Zhang and H. D. Pfister. Compressed sensing and linear codes over real numbers. In *Proc. 2008 Workshop on Inform. Theory and Appl.*, UCSD, La Jolla, CA, February 2008.

[30] F. Zhang and H. D. Pfister. List-message passing achieves capacity on the q-ary symmetric channel for large q. submitted to *IEEE Trans. on Inform. Theory* also available in Arxiv preprint cs.IT/0806.3243, 2008.

[31] F. Zhang and H. D. Pfister. On the iterative decoding of high rate LDPC codes with applications in compressed sensing. in preparation, 2008.