On Pseudocodewords and Decision Regions of Linear Programming Decoding of HDPC Codes

Asi Lifshitz and Yair Be'ery Senior Member, IEEE Tel Aviv University, School of Electrical Engineering Ramat Aviv 69978, ISRAEL

Email: asilifsh@post.tau.ac.il, ybeery@eng.tau.ac.il

Abstract

In this paper we explore the decision regions of Linear Programming (LP) decoding. We compare the decision regions of an LP decoder, a Belief Propagation (BP) decoder and the optimal Maximum Likelihood (ML) decoder. We study the effect of minimal-weight pseudocodewords on LP decoding. We present global optimization as a method for finding the minimal pseudoweight of a given code as well as the number of minimal-weight generators. We present a complete pseudoweight distribution for the [24, 12, 8] extended Golay code, and provide justifications of why the pseudoweight distribution alone cannot be used for obtaining a tight upper bound on the error probability.

Index Terms

Belief propagation, bounded distance decoding, generators, global optimization, linear programming, LP relaxation, pseudocodewords, pseudoweight.

I. INTRODUCTION

The behavior of the BP [1] decoder for the case of finite-length codes does not have simple characteristics, and can be very hard to predict. Linear programming is a well-studied discipline that provides efficient analysis tools. The relationship between linear programming decoding and belief propagation decoding was observed and characterized [2], and the decision regions of these decoders are suggested to be tightly related.

The LP decoder receives the channel likelihood ratios which define an objective function, for which it finds an optimal solution that satisfies a set of constraints. These constraints are inequalities arisen from a given parity check matrix and form a polytope, also known as the *fundamental polytope* [3]. The fundamental polytope is a relaxation of the codewords polytope. It has a clear geometrical representation which is well-suited for finite-length analysis. The vertices of the fundamental polytope are every codeword, but also some non-codewords pseudocodewords [4]. The *fundamental cone* [3] is the conic hull of the fundamental polytope. It has a vertex in the origin, and its edges are also referred to as *minimal pseudo-codewords* [3] or *generators* [5]. The fundamental cone has a more compact representation than the fundamental polytope, and it is sufficient to consider the fundamental cone for evaluating the performance of the LP decoder [5].

The output of the LP decoder is always a vertex of the polytope which maximizes the channel likelihood ratios function. One of the most appealing properties of the LP decoder is the *ML certificate* property - whenever it returns an integral solution, the solution is guaranteed to be the ML codeword; otherwise an error is invoked. There are rare cases [6] for which the vertices of the polytope are codewords only, and in these cases the output of the LP decoder is identical to the output of the ML decoder. In these rare cases a polynomial-time ML decoding is attainable. However, for most cases, and when applied to good error-correcting codes, the LP decoder will suffer from decoding failures due to the presence of pseudocodewords.

The minimal *pseudoweight* [3] of a pseudocodeword in LP decoding is the appropriate analog of the minimal Hamming weight in ML decoding. Furthermore, the minimum Hamming weight is known to be lower bounded by the minimal pseudoweight [7]. There are cases where the minimal pseudoweight equals the minimal Hamming weight, and in these cases, the existence of pseudocodewords may have a minor or even a negligible effect on the decoder's optimality.

High Density Parity Check (HDPC) codes are characterized by a dense parity check matrix. Linear classical codes have a dense parity check matrix by design, which makes them less suitable for LP decoding. The denser the parity check matrix is the more vertices the fundamental polytope will have. Keeping in mind that the number of codewords of a given code is constant, one can realize that increasing the number of vertices is equivalent to increasing the number of pseudocodewords which are not codewords. The BP algorithm is often in use for decoding low-density parity-check (LDPC) codes, for which it has both low complexity and good performance. Its low complexity is achieved due to the fact that the algorithm operates locally on a so-called *Tanner graph* [8] representation of the parity-check matrix. However, operating locally leads to a fundamental weakness of the algorithm - it may fail to converge due to non-codewords pseudocodewords. These pseudocodewords are valid assignments of the *computation tree* [8] of the given code and decoder. Kelley and Sridhara [9] have proved that the pseudocodewords of the computation tree are a superset of the pseudocodewords which lie in the aforementioned fundamental polytope.

The decision regions of a decoding algorithm provide a visualization of the decoder's decisions upon receiving channel signals. They provide a better intuition of the decoder operation, and can be used for comparing different decoding algorithms. The existence of pseudocodewords in iterative decoding and their effect on the decision regions were studied in [3], [10]. In the present work we examine the effect of pseudocodewords on the decision regions and on the performance of the LP decoder.

Presenting a complete picture of the decision regions is usually impossible even for shortlength codes, due to the number of dimensions involved in each decoded signal. Nevertheless, performing cuts in the signal space can provide a clear picture of specific decision regions, which illustrate the effect of pseudocodewords on the performance of the BP and LP decoders.

In order to illustrate the different decision regions of the BP, LP and ML decoders, the [8, 4, 4] extended Hamming code was chosen. It is known that both BP and LP decoders are affected by the selection of the parity check matrix, therefore three different representations for the aforementioned code were chosen.

The contribution of this paper is in providing a better understanding of the LP decoder operation. Global optimization is proposed as a method for finding the minimal weight generators of a given parity check matrix. The paper also presents the difficulties in obtaining a tight LP union bound, based on the generators' weight distribution, and explores the effect of minimal-weight pseudocodewords on the decision regions of the LP decoder.

The rest of the paper is organized as follows: We provide some background on decision regions and a method to produce the decision regions in Section II. In Section III we present the different effect of minimal-weight pseudocodewords on LP decoding. A global optimization

approach for finding the minimal weight generators is described in Section IV. In Section V we presents an LP union bound based on the generators' weight distribution. Section VI concludes the paper.

II. MAPPING OF DECISION REGIONS

The major difficulty of presenting the decision regions of a code longer than three is how to project or reduce an *n*-dimensional space to a two or three dimensional subspace. In this paper the *n*-dimensional space is sliced to a two-dimensional Euclidian subspace. A two dimensional subspace or a *cut* is a plane that is spanned by two orthogonal vectors.

Consider transmitting an *n*-dimensional signal over an AWGN channel, such that the observed data is $\mathbf{r} = \mathbf{s} + \mathbf{n}$ where \mathbf{s} is the transmitted signal, and \mathbf{n} is a normally distributed noise with zero mean and variance σ^2 . The decision regions $\{Z_1, \ldots, Z_M\}$ are the subsets of the signal space \mathbb{R}^n defined by

$$Z_i = \{ \mathbf{r} : p(\mathbf{s}_i | \mathbf{r}) > p(\mathbf{s}_j | \mathbf{r}) \ \forall i \neq j, \ 1 \le i, j \le M \}$$
(1)

where M is the number of codewords.

The decision boundaries are all the points for which exists $\mathbf{r} \in \mathbb{R}^n$ such that $p(\mathbf{s}_i | \mathbf{r}) = p(\mathbf{s}_j | \mathbf{r})$. The decision boundaries divide the signal space into M disjoint decision regions, each of which consists of all the point in \mathbb{R}^n closest in Euclidian distance to the received signal \mathbf{r} . An ML decoder finds which decision region Z_i contains \mathbf{r} , and outputs the corresponding codeword $\hat{\mathbf{c}}_i$. The existence of pseudocodewords in BP and LP decoders divides the signal space into more decision regions than those created solely by codewords. Clearly, these pseudocodewords reduce the decision regions of the codewords, hence deteriorate the decoder optimality.

The first step towards mapping the decision regions is to decide of the two spanning vectors \mathbf{n}_y and \mathbf{n}_x ($\mathbf{n}_y, \mathbf{n}_x \in \mathbb{R}^n$). These two vectors must be orthogonal in order to have a clear 2-dimensional picture, rather than a folded one. The sum of these two vectors is the noise vector that is added to the transmitted signal. The noisy samples are then decoded, and the output of the decoder is recorded along with the received signal. All the received signals which share the same output designate a decision region. In the following the LP decoder uses a C-symmetric

polytope [4] under a binary-input memoryless symmetric channel, thus one may assume without loss of generality that the all-zero codeword was transmitted. For BP and ML decoders, the conditional decoding error probability is independent of the codeword that was sent. Therefore, our analysis will assume that the all-zero codeword was transmitted over an AWGN channel using a BPSK modulation. The BP decoder being used is a sum-product decoder, configured to perform 50 decoding iterations.

In LP decoding, the vertices of the fundamental polytope are a superset of the codewords. While the set of codewords are dominated by the code itself, the set of pseudocodewords is dominated by the relaxation being used. Let C be a binary code $C \in \{0,1\}^n$ and let $\mathcal{V}(\mathcal{P})$ be the set of vertices of the polytope \mathcal{P} . The polytope contains every codewords, but also some fractional pseudocodewords, thus:

$$\mathcal{C} \subseteq \mathcal{V}(\mathcal{P}) \subseteq \mathcal{P} \subseteq [0,1]^n.$$
⁽²⁾

The mapping of a vertex onto a point in a Euclidian plane is performed using the *effective* squared Euclidian distance [11] between a codeword c and a pseudocodeword p in a balanced computation tree:

$$d_{eff}^{2}(\mathbf{c}, \mathbf{p}) = \frac{(\|\mathbf{d}^{2}\| + \sigma_{p}^{2})^{2}}{\|\mathbf{d}^{2}\|}$$
(3)

where $\mathbf{d} = \mathbf{c} - E[\mathbf{p}]$ and $\sigma_p^2 = E[||\mathbf{p}||^2] - ||E[\mathbf{p}]||^2$. If the all-zero codeword is transmitted using a BPSK modulation, then (3) is simplified to

$$d_{eff}^2(\mathbf{0}, \mathbf{p}) = 4w_{eff}(\mathbf{p}) \tag{4}$$

where w_{eff} is the effective Hamming weight in an AWGN channel, given by

$$w_p^{AWGNC}(\mathbf{p}) = w_{eff}(\mathbf{p}) \equiv \frac{\|\mathbf{p}\|_1^2}{\|\mathbf{p}\|_2^2} = \frac{(\sum_{i=1}^n p_i)^2}{\sum_{i=1}^n p_i^2}.$$
(5)

Eq. (5) is sometimes referred to as the *pseudoweight* [3] of **p** in an AWGN channel. The performance of iterative decoders is influenced mostly by the minimal weight pseudocodewords [7], [12], [13], [14], while the ML decoder is influenced mostly by the code minimal Hamming weight. This is why the performance of an ML decoder is not affected by the selection of the

parity check matrix representation, which is not true for the case of BP and LP decoders. If all codewords are chosen with equal probability, then the effective Euclidian distance between the all-zero codeword and the decoded word is d_{eff} . The decision boundary between the all-zero codeword and the decoded word is exactly $\frac{d_{eff}}{2}$ from the origin.

The mapping of the decision regions within a two-dimensional cut is performed as follows:

- 1: Set the y-Axis to represent n_y , and the x-Axis to represent n_x
- 2: Find the normalization factor for n_y and n_x :

$$norm_n_y = \sqrt{\sum_{i=1}^n (\mathbf{n}_{y_i})^2}, \ norm_n_x = \sqrt{\sum_{i=1}^n (\mathbf{n}_{x_i})^2}$$
(6)

3: for y in range *min_added_noise* to *max_added_noise* do

4: for x in range *min_added_noise* to *max_added_noise* do

5: Set the received signal

$$\mathbf{r} = Modulate(\mathbf{0}) + \frac{\mathbf{n}_y \cdot y}{norm_n_y} + \frac{\mathbf{n}_x \cdot x}{norm_n_x}$$
(7)

6: Decode the signal

7: end for

8: end for

9: Map the entire space spanned by y and x to the decoded words.

Normalization of \mathbf{n}_y and \mathbf{n}_x is required in order to maintain a Euclidian space. A unitstep in the direction of \mathbf{n}_y is a step for which the noise that is added in the direction of \mathbf{n}_y will shift the transmitted signal by $\sqrt{\sum_{i=1}^n (\mathbf{n}_{y_i})^2}$ from the origin. The *min_added_noise* and the *max_added_noise* are the two endpoints of both \mathbf{n}_y and \mathbf{n}_x , and are taken such that *min_added_noise* $\geq -\frac{d_{min}}{2}$ and *max_added_noise* $\leq d_{min}$, where d_{min} is the code minimal Hamming distance.

In the following the decision regions of the [8, 4, 4] extended Hamming code are studied. The [8, 4, 4] extended Hamming code is well-suited for studying the decision regions of the BP and LP decoders. It is a self-dual code which has a simple parity check matrix representation with minimal pseudoweight equals d_{min} , but also a representation with pseudoweight equals 3. In order to gain a better understanding of the tight relation between the selected parity check matrix, the decision regions and the decoder's performance, three different parity check matrices are investigated (8), (9), (10). These matrices were originally introduced by Halford and Chugg in [15], for which they also presented the pseudoweight spectra.

$$H_{1} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$
(8)
$$H_{2} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$
(10)

Fig. 1 presents the performance and the weight distribution of the three representations of the [8, 4, 4] extended Hamming code. Fig. 1(a) compares the frame error rate of the LP and BP



(b) Pseudoweight spectra

Fig. 1. Different representations of the [8, 4, 4] extended Hamming code.

decoders using the parity check matrices of (8), (9) and (10). The performance difference between the LP and BP decoders is consistent for the 3 representations, in which the LP decoder slightly outperforms the performance of the BP decoder. Both decoders achieve the best performance when using H_3 and worst performance when using H_1 . Furthermore, the LP decoder has almost the same performance as the ML decoder when using H_3 .

Fig. 1(b) illustrates the pseudoweight distribution of H_1 , H_2 and H_3 . These results are similar to the ones presented in [15]. A first observation is that $w_{p,min}^{AWGNC}(H_3) = d_{min} = 4$, which



Fig. 2. Decision regions of H_1 with $\mathbf{n}_y = (0, 2/3, 2/3, 2/3, 0, 0, 0, 0)$ and $\mathbf{n}_x = (0, 0, 0, 0, 1, 1, 1, 1)$.



Fig. 3. Decision regions of H_3 with $\mathbf{n}_y = (0, 2/3, 2/3, 2/3, 0, 0, 0, 0)$ and $\mathbf{n}_x = (0, 0, 0, 0, 1, 1, 1, 1)$.

can provide an explanation of why the suboptimal LP decoder is almost optimal. A second observation is that H_1 has many more low-weight pseudocodewords compares to H_2 , which is consistent with the performance difference between the two representations.

Fig. 2 and Fig. 3 illustrate some of the decision regions that were found by mapping the decision regions. The solid black lines represent the optimal decision regions of the ML decoder. The bottom left decision region represents the transmitted all-zero codeword. The decision region on its right (if any) represents another codeword which is a linear combination of n_y and n_x that lies in the same plane. The output of an ML decoder can only be a codeword; hence the

region above the solid lines is a region of codewords which are not a linear combination of n_y and n_x . The soft output of the BP decoder enters a hard decision decoder to maintain a binary vector.

Fig. 2 illustrates the decision regions in the plane spanned by $\mathbf{n}_y = (0, 2/3, 2/3, 2/3, 0, 0, 0, 0)$ and $\mathbf{n}_x = (0, 0, 0, 0, 1, 1, 1, 1)$. Clearly, the decision boundary between \mathbf{c}_0 and \mathbf{c}_1 obeys the $\frac{d_{min}}{2}$ rule. In the direction of \mathbf{n}_y , the decision boundary of the ML decoder is beyond $\frac{d_{min}}{2}$, since there is no competing codeword in this direction. The word \mathbf{p}_0 in Fig. 2(a) is a pseudocodeword, since it is fractional and has a weight equals 3 which is smaller than d_{min} . Fig. 2(a) also illustrates how the minimal-weight pseudocodeword \mathbf{p}_0 deteriorates the decoder's optimality by reducing the decision region of the transmitted codeword.

Fig. 2(a) and Fig. 2(b) show that BP and LP decoders share the same decision boundaries between \mathbf{c}_0 and \mathbf{c}_1 , and same boundaries between \mathbf{c}_0 and \mathbf{p}_0 . The location of \mathbf{p}_0 in Fig. 2(a) is $d_{eff}(\mathbf{0}, \mathbf{p}_0) = \sqrt{4w_p(\mathbf{p}_0)} = \sqrt{4\frac{(2/3+2/3+2/3)^2}{(2/3)^2+(2/3)^2+(2/3)^2}} = \sqrt{12}$ from \mathbf{c}_0 . The same calculation holds for Fig. 2(b): $d_{eff}(\mathbf{0}, \mathbf{p}_0) = \sqrt{4w_p(\mathbf{p}_0)} = \sqrt{4\frac{(1+1+1)^2}{(1)^2+(1)^2+(1)^2}} = \sqrt{12}$. The decision boundaries are exactly at $\frac{d_{eff}}{2} = \frac{\sqrt{12}}{2} = \sqrt{3}$ from \mathbf{c}_0 . Since the decision boundary is smaller than $\frac{d_{min}}{2}$, the LP and BP decoders are not bounded distance [17], [18] decoders. The difference between BP and LP decoders is in the decision regions of pseudocodewords, and is caused due to the different algorithms that are used. While the decision regions of the LP decoder are convex polytopes [16], their counterparts in BP decoding are non-convex and more chaotic. Clearly, the decision regions of \mathbf{p}_0 and \mathbf{p}_1 in BP decoding are larger than their counterparts in LP decoding. Nevertheless, from this figure it is clear that this difference has no major impact on the performance.

 space is sometimes misleading, due to the information loss caused by the hard decision at the output of the BP decoder. This is why we omitted the position of p_0 and p_1 from Fig. 3(b). The fact that the decision regions of p_0 and p_1 in BP decoding are much larger than those of the LP decoder does not necessarily reflected in the performance, since the majority of the area is located outside the optimal decision region of c_0 , i.e. in the error region.

III. THE EFFECT OF MINIMAL WEIGHT PSEUDOCODEWORDS ON LP DECODING

Simulations show that although the performance of the LP decoder is dominated by lowweight pseudocodewords, not all low-weight pseudocodewords have the same contribution to the error probability. In this section we will justify why some minimal weight pseudocodewords may have a higher contribution to the error probability compared to others. We will base our justification on both simulation results and decision regions.

The polytope of H_1 has 26 vertices of pseudoweight equals 3. Our simulation results for different SNRs show, for example, that the pseudocodeword $\mathbf{p}_0 = (0, 2/3, 2/3, 2/3, 0, 0, 0, 0)$ causes approximately 4 times more decoding errors than $\mathbf{p}_1 = (1, 0, 0, 0, 0, 1/3, 1/3, 1/3)$. There are several properties that affect the error probability of a given pseudocodeword. When listing all pseudocodewords, one can see that there are many pseudocodewords with support equals 4 that share 3 out of 4 non-zero components with \mathbf{p}_1 . It means that in the objective function the selection between such candidates depends on two independent random variables. However, there are no pseudocodewords with support equals 3 that share 2 components out of 3 with \mathbf{p}_0 . There are pseudocodewords with support higher than 3 that contain non-zero components in the same positions as \mathbf{p}_0 but with lower values. Such components have weaker effect on the cost value, and lead to fewer decoding errors.

We will now present a cut that contains the aforementioned \mathbf{p}_0 and \mathbf{p}_1 , and show that in the specific cut the decision region of \mathbf{p}_0 is larger than that of \mathbf{p}_1 , which provide another perspective of why \mathbf{p}_0 causes more decoding errors. Fig. 4 presents a cut created by the noise vectors $\mathbf{n}_y = (0, 2/3, 2/3, 2/3, 0, 0, 0, 0)$ and $\mathbf{n}_x = (1, 0, 0, 0, 0, 1/3, 1/3, 1/3)$. Notice that the decision regions, at least in the presented cut, have a different behavior as illustrated in Fig. 4(a). While the decision region of \mathbf{p}_1 increases only in the y-axis, the decision region of \mathbf{p}_0 grows in both axes.



Fig. 4. Decision regions of an LP decoder with $\mathbf{n}_y = (0, 2/3, 2/3, 2/3, 0, 0, 0, 0)$ and $\mathbf{n}_x = (1, 0, 0, 0, 0, 1/3, 1/3, 1/3)$.

13

DRAFT

The existence of \mathbf{p}_0 and \mathbf{p}_1 in the polytope of H_1 reduces the decision region of \mathbf{c}_0 as shown in Fig. 4(a). The polytope of H_2 does not contain \mathbf{p}_1 , thus the decision region of \mathbf{c}_0 is bigger than that of H_1 as presented in Fig. 4(b). The fundamental polytope of H_3 does not contain \mathbf{p}_0 , nor \mathbf{p}_1 , thus the decision region of \mathbf{c}_0 is identical to that of the optimal ML decoder, as can be seen from Fig. 4(c).

IV. FINDING THE MINIMAL WEIGHT GENERATORS

Inspired by the work of [16] we were encouraged to seek for a deterministic approach for finding the minimal weight generators. The heuristic method of [16] provides an excellent upper bound on the minimal pseudoweight, and it can be used for long and dense codes. It still lacks the certificate that the minimal weight generator that was found using this method is the minimal weight generator of a given parity check matrix. The number of iterations that are needed to reach a tight bound is also left open. The number of minimal weight generators is fundamental for obtaining a union bound, but the method of [16] can only estimate this number.

In this section we present a method for finding the minimal weight generator of a given parity check matrix, as well as the number of minimal weight generators.

Proposition 1. ([9]) The pseudoweight is invariant under scaling.

Proof: We need to prove that $w_p^{AWGNC}(\alpha \mathbf{p}) = w_p^{AWGNC}(\mathbf{p})$ where α is a real positive number, and $\mathbf{p} \in \mathbb{R}^n$ is a pseudocodeword.

$$w_p^{AWGNC}(\alpha \mathbf{p}) = \frac{\left(\sum_{i=1}^n \alpha p_i\right)^2}{\sum_{i=1}^n (\alpha p_i)^2} = \frac{\alpha^2 \left(\sum_{i=1}^n p_i\right)^2}{\alpha^2 \sum_{i=1}^n (p_i)^2} = w_p^{AWGNC}(\mathbf{p}).$$
 (11)

Given a binary parity check matrix $H \in \mathbb{F}_2^{m \times n}$, the fundamental cone $\mathcal{K} \stackrel{\Delta}{=} \mathcal{K}(H)$ is defined as the conic hull of the fundamental polytope P(H), and can be described by the following set of linear inequalities:

$$\mathcal{K} = \left\{ \mathbf{p} \in \mathbb{R}^n \middle| \begin{array}{l} p_i \ge 0 \text{ and} \\ \sum_{i=1, i \ne i'}^n h_{ji} p_i \ge h_{ji'} p_{i'} \\ \forall \ 1 \le i \le n, \ \forall \ 1 \le j \le m \end{array} \right\}$$
(12)

where h_{ji} denotes the entry of H in the *j*th row and *i*th column.

Corollary 2. All points on an edge of the fundamental cone have the same pseudoweight.

Proof: Let \mathbf{a} and \mathbf{b} be two points on the edge $E_i \in \mathcal{K}$. From the definition of \mathcal{K} it is clear that each edge is a ray with an endpoint at the origin. Being on the same ray, one can express $\mathbf{a} = \alpha \mathbf{b}$ where α is a real positive number. From Proposition 1 it follows that \mathbf{a} and \mathbf{b} have the same pseudoweight.

Searching for the minimal weight generator is equivalent to searching for the minimal weight edge of the fundamental cone \mathcal{K} . We will now prove that for searching for the minimal weight edge one can bound \mathcal{K} and use the following polytope:

$$\mathcal{P}_{\mathcal{K}} = \left\{ \mathbf{p} \in \mathbb{R}^{n} \middle| \begin{array}{l} p_{i} \geq 0 \text{ and} \\ \sum_{i=1}^{n} p_{i} = a, \ a > 0 \\ \sum_{i=1, i \neq i}^{n} h_{ji} p_{i} \geq h_{ji'} p_{i'} \\ \forall 1 \leq i \leq n, \forall 1 \leq j \leq m \end{array} \right\}$$
(13)

where the essence of the constant $a \in \mathbb{R}$ is to increase the dynamic range of the problem and prevent scaling issues in optimization softwares.

Proposition 3. The edges of \mathcal{K} and the vertices of $\mathcal{P}_{\mathcal{K}}$ have the same weight distribution.

Proof: Let E_i be an edge of \mathcal{K} and let \mathbf{p} be an arbitrary point on E_i . From (13) it is clear that E_i is also an edge of $\mathcal{P}_{\mathcal{K}}$. Suppose $\sum_{i=1}^n p_i = b$, and let $k = \frac{a}{b}$, then according to (11) the pseudocodeword $\mathbf{p}' = k\mathbf{p}$ has the same weight as \mathbf{p} and the sum of its components is a; Thus \mathbf{p}' is a vertex of $\mathcal{P}_{\mathcal{K}}$. Now, let E_j be an edge of $\mathcal{P}_{\mathcal{K}}$. From the definition of $\mathcal{P}_{\mathcal{K}}$, E_j has two endpoints: One in the origin and one in $\tilde{\mathbf{p}}$ for which $\sum_{i=1}^n \tilde{p}_i = a$. Clearly, \mathcal{K} has an edge with an endpoint in the origin, that passes through $\tilde{\mathbf{p}}$ and goes off to infinity. According to Corollary 2 the pseudoweight of this edge in \mathcal{K} is the same as the vertex $\tilde{\mathbf{p}} \in \mathcal{P}_{\mathcal{K}}$, which completes the proof.

The problem of finding the minimal weight in an AWGN channel becomes:

$$w_{p_{min}} = \min_{\mathbf{p} \in \mathcal{P}_{\mathcal{K}}} w_p(\mathbf{p}) = \min_{\mathbf{p} \in \mathcal{P}_{\mathcal{K}}} \frac{(\sum_{i=1}^n p_i)^2}{\sum_{i=1}^n (p_i)^2} = \min_{\mathbf{p} \in \mathcal{P}_{\mathcal{K}}} \frac{a^2}{\sum_{i=1}^n (p_i)^2}$$
(14)

15

where the last equation follows from the definition of $\mathcal{P}_{\mathcal{K}}$. Being a constant, *a* does not affect the minimization process, thus instead of solving (14) one may consider solving the following simpler maximization problem:

$$\max_{\mathbf{p}\in\mathcal{P}_{\mathcal{K}}}\sum_{i=1}^{n}(p_{i})^{2}.$$
(15)

The minimal pseudoweight $w_{p_{min}}$ is simply the division of a^2 by the optimal solution of (15).

The maximization problem of (15) is non-convex and may have several local maxima. Algorithms for solving such problems are termed *Global Optimization* and are able to find the global solution in the presence of multiple local solutions.

Global optimization algorithms are usually divided into deterministic and probabilistic approaches. The solution of a deterministic approach is guaranteed to be the global solution, or at least a local solution which differs from the global solution by less than a given $\epsilon > 0$. Probabilistic algorithms require a shorter runtime compares to deterministic ones, but their solution may not be the global optimum.

An efficient deterministic approach for solving global optimization problems is the *Branch and Bound* algorithm. The algorithm relies on the existence of a convex relaxation of the original problem [19], whose optimal solution provides a lower bound on the solution of the original

Code	$w_{\rm p_{min}}$	$N_{\rm p_{min}}$
Hamming [15, 11, 3]	3.0	127
Hamming [31, 26, 3]	3.0	1185
BCH [31, 21, 5]	3.0	6
BCH [63, 45, 7]	3.0	1
BCH [63, 39, 9]	3.299176	1
BCH [63, 36, 11]	3.2	83
BCH [127, 113, 5]	3.0	134
BCH [127, 64, 21]	3.0	2
BCH [255, 131, 37]	3.33333	9
Tanner [155, 64, 20]	16.403683	465

 TABLE I

 MINIMAL-WEIGHT AND NUMBER OF MINIMAL-WEIGHT GENERATORS

problem.

The simplest probabilistic global optimization algorithm is the *Multistart* algorithm, which uses a local algorithm starting from several points distributed over the whole optimization region. The local optimum with the best objective value is taken as the global solution.

Some global optimization softwares such as *BARON* (Branch And Reduce Optimization Navigator) [20] can also provide the *k*-best solutions, or all local solutions, which guarantee not only finding the minimal weight, but also the distribution of the minimal weight generators.

Being deterministic and efficient, BARON was chosen as the global optimization software. The minimal weight along with the number of minimal weight generators $N_{p_{min}}$ for several selected codes are presented in Table I. We performed short cycles reduction [15] on the BCH codes to improve their performance under iterative decoding. The minimal pseudoweight for the [155, 64, 20] Tanner code [21] presented in [12] is $d_{LP} \approx 16.4037$, which is similar to our results. Notice that the LDPC Tanner code has a minimal pseudoweight much higher than all the tested HDPC codes. Although short cycles were removed from the BCH codes, we were not able to increase the minimal pseudoweight beyond $3\frac{1}{3}$. It is interesting to develop new methods for increasing the minimal pseudoweight of a given dense parity check matrix without adding redundant parity checks.

V. LP UNION BOUND

A union bound for LP decoding was mentioned in [14], [22] and [23], but a full characterization of such a bound was not provided. In this section we examine the [8, 4, 4] Extended Hamming code and the [24, 12, 8] extended Golay code, and present why calculation of such a bound is not an easy task.

The ML union bound [24] for the case where the all-zero codeword s_0 is transmitted is

$$Pr[error|\mathbf{s}_0] \le \sum_{i=1}^{M-1} Q\left(\frac{d_{0i}}{2\sigma}\right)$$
(16)

where M is the number of signals and d_{0i} is the distance between s_0 and s_i . Clearly, (16) can be very loose in case the individual events are not disjoint. For large SNRs the union bound of (16) can be approximated by including only the dominating terms:

$$Pr[error|\mathbf{s}_0] \approx N_{min}Q\left(\frac{d_{min}}{2\sigma}\right)$$
 (17)

where N_{min} is the number of nearest neighbors of the transmitted signal s_0 . We can no longer assume that (17) is an upper bound, since we've neglected positive terms from (16).

Assuming that the all-zero codeword is transmitted, the error probability over the fundamental polytope is equal to that over the fundamental cone [5]; Thus, a union bound for the LP decoder can be formulated from (16) as follows:

$$Pr[error|\mathbf{s}_0] \le \sum_{i=1}^{N_p - 1} Q\left(\frac{w_{p_i}}{2\sigma}\right)$$
(18)

where N_p is the number of generators and w_{p_i} is the pseudoweight of generator *i*. Similarly, we can obtain an approximation for large SNRs:

$$Pr[error|\mathbf{s}_0 \ transmitted] \approx N_{p_{min}} Q\left(\frac{w_{p_{min}}}{2\sigma}\right)$$
(19)

where $N_{p_{min}}$ is the number of minimal weight generators, and $w_{p_{min}}$ is the minimal pseudoweight.

In the following we will use the parity check matrices of (8), (9) and (10) for the Extended [8, 4, 4] Hamming code and (20), (21) for the [24, 12, 8] extended Golay code.

The parity check matrices for the [24, 12, 8] extended Golay code were introduced by Halford in [25]. The parity check matrix in (21) was obtained by applying short cycles reduction [15] on (20). The Tanner graph representation of H_G contains 1,551 4-cycles and 65,632 6-cycles, while there are 295 4-cycles and 6,204 6-cycles in the representation of $H_{G'}$. It was shown in [25] that the message passing algorithm using $H_{G'}$ outperforms the one using H_G by more than 1 dB.

From Section III, it is clear why having a tight LP upper bound is a complicated task: In the low SNR regime the bound may be very loose if not scaling each minimal weight pseudocodeword by its contribution to the error probability. In the high SNR regime, especially for medium and long codes, the minimal weight pseudocodewords may have low-volume decision regions, thus may have a negligible effect on the performance of the LP decoder. A similar phenomenon was observed in [17], [18] for *pseudo nearest neighbors* in bounded-distance decoding algorithms. In [18] Fishler et al. derived an approximated probability ratio between the error contribution of a non-codeword neighbor and a codeword nearest neighbor. The ratio was calculated based on the ratio between the volumes of the decision regions of the two competitive neighbors. Incorporating this ratio yielded a better approximation for an upper bound.



(b) [24, 12, 8] extended Golay code

Fig. 5. Weight distribution of the [8, 4, 4] extended Hamming code and the [24, 12, 8] extended Golay code.

Fig. 5 presents the generators' weight distribution of the [8, 4, 4] extended Hamming code and the [24, 12, 8] extended Golay code. Clearly, using (18) as an upper bound for the LP decoder will result an error probability much higher than unity, which makes the bound useless. The reason is that the large number of generators leads to many joint events, which make the bound very loose. Strictly speaking, while the [24, 12, 8] extended Golay code has 4096 codewords, there are 91,113,330 and 231,146,334 generators for H_G and $H_{G'}$, respectively. It was mentioned above that $H_{G'}$ was obtained from H_G by applying short cycles reduction. Notice that not only $H_{G'}$ has a higher minimal pseudoweight, but its entire pseudoweight spectra is centered to the right of the one of H_G , as illustrated in Fig. 5(b).

Code	Parity Check Matrix	$w_{\rm p_{\rm min}}$	$\mathbf{N}_{\mathbf{p}_{\min}}$
Extended Hamming [8, 4, 4]	H_1	3.0	26
	H_2	3.0	4
	H_3	4.0	14
Extended Golay [24, 12, 8]	H_G	3.0	2
	$H_{G'}$	3.6	2

TABLE II

MINIMAL-WEIGHT GENERATORS OF THE [8, 4, 4] extended Hamming code and the [24, 12, 8] extended Golay code

Table II presents the number of minimal-weight generators of the aforementioned parity check matrices. The pseudoweights from Table II were used to calculate the LP Union Bound Approximation (UBA) of (19). The results are presented in Fig. 6. For clarity the actual error probabilities are also presented. The performance of the LP decoder for the chosen matrices are correlated with the generators' weight distribution that was presented in Fig. 5. From Fig 6(a) one can see that the suggested UBA is tight for H_1 and H_3 , but inaccurate for H_2 . The UBA is much worse for the case of the extended Golay code, as presents in Fig. 6(b). In this case the UBA does not reflect the actual behavior of the decoder, but rather presents a too-optimistic behavior. The reason is due to the fact that there are only two minimal-weight generators for both representations, whereas the ML UBA (17) employs 759 nearest neighbors. Notice that there are 91,113,326 and 230,918,045 generators of pseudoweight lower than d_{min} for H_G and $H_{G'}$, respectively. Had we considered all the generators having pseudoweight lower than d_{min}



(b) [24, 12, 8] extended Golay code

Fig. 6. LP UBA for different representations of the [8, 4, 4] extended Hamming code and the [24, 12, 8] extended Golay code.

23

in (19), we would have gained an LP UBA higher than unity. The LP UBA does not have a coherent behavior, i.e. the bound can be sometimes below the actual performance curve, which again disqualifies it as an upper bound or as an approximation.

The pseudoweight and the weight-distribution are not enough for implementing a tight LP upper bound. A tight and accurate bound must take the volume of the decision regions into account. As was presented, some low-weight pseudocodewords which have small volume have also small effect on the decoder's performance, but are very dominant in the equation of the LP union-bound. A tight LP union-bound must have a distinction between codewords and different types of pseudocodewords.

VI. CONCLUSION

The decision regions of the LP decoder were studied and compared to those of the BP and ML decoders. We showed that both BP and LP are not bounded distance decoders. The different effect of minimal-weight pseudocodewords on the performance of the LP decoder was examined. Global optimization was presented as a method for finding the minimal pseudoweight, as well as the number of minimal weight generators. An LP union bound was presented, along with an explanation of why having the pseudoweight spectra is not sufficient for finding a tight bound. Finding the ratio between the error contribution of a nearest pseudocodeword and a nearest codeword will tighten the union bound, and is left open for further research.

REFERENCES

- [1] F. R. Kschischang, B. J. Frey, and H.-A. Loeliger, "Factor graphs and the sum-product algorithm," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 498–519, Feb. 2001.
- [2] P. O. Vontobel and R. Koetter, "On the relationship between linear programming decoding and min-sum decoding," in Proc. IEEE International Symposium on Information Theory and its Applications, Parma, Italy, Oct. 2004.
- P. O. Vontobel and R. Koetter, "Graph-cover decoding and finite-length analysis of message-passing iterative decoding of ldpc codes," 2005. [Online]. Available: http://www.arxiv.org/abs/cs.IT/0512078
- [4] J. Feldman, M. J. Wainwright, and D. R. Karger, "Using linear programming to decode binary linear codes," *IEEE Trans. Inf. Theory*, vol. 51, no. 1, pp. 954–972, Jan. 2005.
- [5] P. Chaichanavong and P. H. Siegel, "Relaxation bounds on the minimum pseudoweight of linear block codes," in Proc. IEEE International Symposium on Information Theory, no. 805-809, Adelaide, Australia, Sep. 4-9 2005. [Online]. Available: http://www.arxiv.org/abs/cs.IT/0508046

- [6] N. Kashyap, "A decomposition theory for binary linear codes," *IEEE Trans. Inf. Theory*, vol. 54, no. 7, pp. 3035–30589, July. 2008.
- [7] P. O. Vontobel and R. Koetter, "Lower bounds on the minimum pseudo-weight of linear codes," in *IEEE International Symposium on Information Theory*, Chicago, IL, USA., June 27-July 2 2004, p. 70.
- [8] N. Wiberg, "Codes and decoding on general graphs," Ph.D. dissertation, Linkoping University, Linkoping, Sweden, 1996.
- [9] C. Kelley and D. Sridhara, "Pseudocodewords of tanner graphs," *IEEE Trans. Inf. Theory*, vol. 53, no. 11, pp. 4013–4038, Nov. 2007.
- [10] B. J. Frey, R. Koetter, and A. Vardy, "Signal space characterization of iterative decoding," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 766–781, Feb. 2001.
- [11] G. D. Forney, Jr., R. Koetter, F. R. Kschischang, and A. Reznik, "On the effective weights of pseudocodewords for codes defined on graphs with cycles," in *Codes, Systems and Graphical Models*, ser. IMA Volumes in Mathematics and Its Applications. New York/Minneapolis: Springer-Verlag, Nov. 1998, vol. 123, pp. 101–112.
- [12] M. Chertkov and M. Stepnov, "An efficient pseudo-codeword-search algorithm for linear programming decoding of ldpc codes," *IEEE Trans. Inf. Theory*, vol. 54, no. 4, pp. 1514–1520, Apr. 2008.
- [13] P. O. Vontobel, R. Smarandache, N. Kiyavash, J. Teutsch, and D. Vukobratovic, "On the minimal pseudo-codewords of codes from finite geometries," in *Proc. IEEE International Symposium on Information Theory*, no. 980-984, Adelaide, Australia, Sep. 4-9 2005. [Online]. Available: http://www.arxiv.org/abs/cs.IT/0508019
- [14] M. Chertkov, "Reducing the error floor," in *Proc. Information Theory Workshop*, no. 230 235, Lake Tahoe, CA, USA, Sep.2-6 2007. [Online]. Available: http://arxiv.org/abs/0706.2926v1
- [15] T. R. Halford and K. M. Chugg, "Random redundant iterative soft-in soft-out decoding," *IEEE Trans. Commun.*, vol. 56, no. 4, pp. 513–517, Apr. 2008.
- [16] M. Chertkov and M. Stepanov, "Polytope of correct (linear programming) decoding and low-weight pseudo-codewords," Feb. 2011. [Online]. Available: http://arxiv.org/abs/1102.3902
- [17] O. Amrani and Y. Be'ery, "Bounded-distance decoding: algorithms, decision regions, and pseudo nearest-neighbors," *IEEE Trans. Inf. Theory*, vol. 44, no. 7, pp. 3072–3082, Nov. 1998.
- [18] E. Fishler, O. Amrani, and Y. Be'ery, "Geometrical and performance analysis of gmd and chase decoding algorithms," *IEEE Trans. Inf. Theory*, vol. 45, no. 5, pp. 1406–1422, 1999.
- [19] N. V. Sahinidis and M. Twarmalani, Convexification and Global Optimization in Continuous and Mixed-Integer Nonlinear Programming. Kluwer Academic Publishers Group, 2002.
- [20] N. V. Sahinidis, "BARON: A general purpose global optimization software package," *Journal of Global Optimization*, vol. 8, pp. 201–205, 1996.
- [21] R. M. Tanner, D. Sridhara, A. Sridharan, T. E. Fuja, and D. J. Costello, "Ldpc block and convolutional codes based on circulant matrices," *IEEE Trans. Inf. Theory*, vol. 50, pp. 2966–2984, 2004.
- [22] R. Smarandache and P. O. Vontobel, "Pseudo-codeword analysis of tanner graphs from projective and euclidean planes," *IEEE Trans. Inf. Theory*, vol. 53, no. 7, pp. 2376–2393, Jul. 2007.
- [23] V. Skachek and M. F. Flanagan, "Lower bounds on the minimum pseudodistance for linear codes with q-ary PSK modulation over AWGN," in *Proc. 5th International Symposium on Turbo Codes and Related Topics*, Lausanne, Switzerland, Sep. 1-5 2008.
- [24] J. R. Barry, E. A. Lee, and D. G. Messerschmitt, Digital Communication, 3rd ed. Springer, 2004.

[25] T. R. Halford, "The extraction and complexity limits of graphical models for linear codes," Ph.D. dissertation, Los Angeles, CA, USA, 2007.