International Symposium on Information Theory and its Applications, ISITA2004
Parma, Italy, October 10–13, 2004

On the Relationship between Linear Programming Decoding and Min-Sum Algorithm Decoding

Pascal O. Vontobel and Ralf Koetter

Coordinated Science Laboratory and Dept. of ECE
University of Illinois at Urbana-Champaign
1308 West Main Street, Urbana, IL 61801, USA
E-mail: vontobel@ifp.uiuc.edu, koetter@uiuc.edu

Abstract

We are interested in the characterization of the decision regions when decoding a low-density parity-check code with the min-sum algorithm. Observations made in [1] and experimental evidence suggest that these decision regions are tightly related to the decision regions obtained when decoding the code with the linear programming decoder. We introduce a family of quadratic programming decoders that aims at explaining this behavior. Moreover, we also point out connections to electrical networks.

1. INTRODUCTION

The main tool of this paper is a theorem by Weiss and Freeman [2, Claim 1] that characterizes the behavior of the min-sum algorithm (MSA) decoder when it converges. Weiss and Freeman actually formulated the theorem for the max-product algorithm (MPA) but the MPA applied to a graphical model representing a global function $\exp(-f(\mathbf{x}))$ and the min-sum algorithm applied to a graphical model representing the global function $f(\mathbf{x})$ do essentially the same computations, so any statement about the MPA can be turned into a statement about the MSA and vice-versa. Note that we define the range of the message functions for the MSA to be not only the real line $\mathbb{R}$ but the extended real line $\mathbb{R} \cup \{-\infty, +\infty\}$ and when we talk about convergence of the MSA we also allow convergence to $\pm\infty$.

Before we can restate the theorem here, we briefly need to introduce the notion of an SLT neighborhood [2, p. 738].

Definition 1 *A* single loops and trees (SLT) *neighborhood of an assignment $\mathbf{x}^*$ in a graphical model*[1] *$\mathcal{G}$ includes all assignments $\mathbf{x}$ that can be obtained from $\mathbf{x}^*$ by the following:*

- *Choosing an arbitrary subset $\mathcal{S}$ of nodes in $\mathcal{G}$ that consists of disconnected combinations of trees and single loops.*
- *Assigning arbitrary values to $\mathbf{x}_{\mathcal{S}}$ – the chosen subset of nodes. The other nodes have the same assignment as in $\mathbf{x}^*$.*

Theorem 2 *Consider an arbitrary graphical model $\mathcal{G}$ with arbitrary potentials whose global function*[2] *we denote by $f(\mathbf{x}, \mathbf{y}) = f(\mathbf{y}) + f(\mathbf{x}|\mathbf{y})$. Here, $\mathbf{x}$ and $\mathbf{y}$ represent unobserved and observed variables, respectively. For a given $\mathbf{y}$ the global function equals a constant plus $f(\mathbf{x}|\mathbf{y})$. Now, if $\mathbf{m}^*$ is a fixed point of the messages of the MSA (applied to $\mathcal{G}$ and with the standard update schedule) and $\mathbf{x}^*$ is the assignment based on $\mathbf{m}^*$ then $f(\mathbf{x}^*|\mathbf{y}) < f(\mathbf{x}|\mathbf{y})$ for all $\mathbf{x} \neq \mathbf{x}^*$ in the SLT neighborhood of $\mathbf{x}^*$.*

Proof: See [2, Claim 1]. □

The above theorem can for example be used to prove an important fact about Gaussian graphical models.

Corollary 3 *For a Gaussian graphical model of arbitrary topology. If belief propagation converges, then the posterior marginal means calculated using belief propagation are exact.*[3]

Proof: See e.g. [2, Cor. 1]. □

Both authors were supported by NSF Grants CCR 99-84515 and CCR 01-05719.

[1] A graphical model here can be a factor graph or one of the graphical models considered in [2].

[2] Here and in the following the global functions will represent *additive* cost functions.

[3] Remember that for Gaussian graphical models belief propagation and MPA are essentially equivalent.

2. NOTATION AND PRELIMINARIES

We let $\mathbb{R}$, $\mathbb{R}_+$, and $\mathbb{R}_{++}$ be the set of real numbers, the set of non-negative real numbers, and the set of positive real numbers, respectively. In the following, all scalars, entries of vectors,[4] and entries of matrices will be considered to be in $\mathbb{R}$, unless noted otherwise. The Galois field with two elements will be denoted by $\mathbb{F}_2$ and the set $\mathbb{F}_2$ will be embedded in the natural way into $\mathbb{R}$. Any binary code $\mathbb{C} \subseteq \mathbb{F}_2^n$ will consequently be seen as a discrete subset of $\mathbb{R}^n$. (Note that $\mathbb{C}$ denotes here a binary code and *not* the set of complex numbers.) Moreover, we will use Iverson's convention, i.e. for a statement A we have $[A] = 1$ if A is true and $[A] = 0$ otherwise. From this we also derive the notation $[\![A]\!] \overset{\triangle}{=} -\log[A]$, i.e. $[\![A]\!] = 0$ if A is true and $[\![A]\!] = +\infty$ otherwise. Let $\mathcal{S}$ be some set. A function like $\mathbb{R}^n \to \mathbb{R}_+ : \mathbf{x} \mapsto [\mathbf{x} \in \mathcal{S}]$ is called an indicator function for the set $\mathcal{S}$, whereas a function like $\mathbb{R}^n \to \mathbb{R}_+ : \mathbf{x} \mapsto [\![\mathbf{x} \in \mathcal{S}]\!]$ is called a neglog indicator function for the set $\mathcal{S}$. Of course, this second function can also be considered as a cost or penalty function.

When representing global functions by factor graphs we will use normal factor graph (also called Forney-style factor graphs, FFGs [3, 4, 5]). Let $f(\mathbf{x})$ be some global function. We say that $\mathbf{x}$ is a valid configuration if $f(\mathbf{x}) < \infty$. (When considering the MPA, a vector $\mathbf{x}$ is a valid configuration if it fulfills $f(\mathbf{x}) > 0$.) Instead of writing "we perform algorithm $\mathcal{A}$ on the graph $\mathcal{G}$" we simply write "$\mathcal{A}_\mathcal{G}$".

Let $\mathcal{S} \subseteq \mathbb{R}^n$ be some set and let $\phi : \mathbb{R}^n \to \mathbb{R}$ be some function. A minimization problem of the form[5] $\hat{\mathbf{x}} = \arg\min_{\mathbf{x} \in \mathcal{S}} \phi(\mathbf{x})$ is equivalent to the minimization problem $\hat{\mathbf{x}} = \arg\min_{\mathbf{x} \in \mathbb{R}^n} [\![\mathbf{x} \in \mathcal{S}]\!] + \phi(\mathbf{x})$. E.g. any standard linear program (LP) $\hat{\mathbf{x}} = \arg\min_{\mathbf{x} \in \mathbb{R}^n : \mathbf{A}\mathbf{x}^\mathsf{T} \leq \mathbf{b}^\mathsf{T}} \mathbf{c}\mathbf{x}^\mathsf{T}$ is equivalent to the minimization problem $\hat{\mathbf{x}} = \arg \min_{\mathbf{x} \in \mathbb{R}^n} [\![\mathbf{A}\mathbf{x}^\mathsf{T} \leq \mathbf{b}^\mathsf{T}]\!] + \mathbf{c}\mathbf{x}^\mathsf{T}$. In order to facilitate the statements in this paper, we will assume that all the minimization problems have a unique minimum.

Remark 4 *Let $g : \mathbb{R}^{n_1} \times \mathbb{R}^{n_2} \to \mathbb{R}$ be a convex function, let $\mathcal{P} = \mathcal{P}_1 \times \mathcal{P}_2 \subset \mathbb{R}^{n_1} \times \mathbb{R}^{n_2}$ where $\mathcal{P}_1 \subset \mathbb{R}^{n_1}$ and $\mathcal{P}_2 \subset \mathbb{R}^{n_2}$ are some convex and closed sets, let $f : \mathbb{R}^{n_1} \times \mathbb{R}^{n_2} \to \mathbb{R}$, $\mathbf{u} = (\mathbf{u}_1, \mathbf{u}_2) \mapsto [\![\mathbf{u}_1 \in \mathcal{P}_1]\!] + [\![\mathbf{u}_2 \in \mathcal{P}_2]\!] + g(\mathbf{u})$, and let $\mathbf{u}^* = (\mathbf{u}_1^*, \mathbf{u}_2^*)$ be a point on the boundary of $\mathcal{P}$. If we can show that $f(\mathbf{u}_1^*, \mathbf{u}_2^*) \leq f(\mathbf{u}_1, \mathbf{u}_2^*)$ for every $\mathbf{u}_1 \in \mathcal{P}_1$ and that $f(\mathbf{u}_1^*, \mathbf{u}_2^*) \leq f(\mathbf{u}_1^*, \mathbf{u}_2)$ for every $\mathbf{u}_2 \in \mathcal{P}_2$ then $f(\mathbf{u}^*) = \min_{\mathbf{u} \in \mathbb{R}^n} f(\mathbf{u})$, i.e. f attains the global minimum at $\mathbf{u}^*$. (This statement can easily be generalized to functions $g : \mathbb{R}^{n_1} \times \cdots \times \mathbb{R}^{n_k} \to \mathbb{R}$ and sets $\mathcal{P}_1, \ldots, \mathcal{P}_k$ for some arbitrary finite k.)*

Proof: (Sketch) Firstly, let us restrict f to the set $\mathcal{P}_1 \times \{\mathbf{u}_2^*\}$: we see that $f(\mathbf{u})$ is globally minimal for this restricted f. Secondly, let us restrict f to the set $\{\mathbf{u}_1^*\} \times \mathcal{P}_2$: we see again that $f(\mathbf{u})$ is globally minimal for this restricted f. This gives us enough information about the first-order behavior of the function f over $\mathcal{P}$ around $\mathbf{u}^*$ to conclude the global minimality of $\mathbf{u}^*$ from the convexity of g. □

[4] Note that all vectors will be *row* vectors.

[5] Note that strictly speaking, arg min returns a set containing all minimum-achieving points. For simplicity, we assume that arg min does not give back this set itself but an element thereof; in the case the set contains more that one element ties will be broken in a consistent fashion.

3. BLOCK-WISE MAXIMUM A-POSTERIORI DECODING OF CODES

We consider the problem of data communication over a noisy channel with the help of a binary code $\mathbb{C} \subseteq \mathbb{F}_2^n$ of length n over $\mathbb{F}_2$. We assume that every codeword $\mathbf{x} \in \mathbb{C}$ is transmitted with equal probability, i.e. $P_\mathbf{X}(\mathbf{x}) = 2^{-nR}$ if $\mathbf{x} \in \mathbb{C}$ and $P_\mathbf{X}(\mathbf{x}) = 0$ otherwise, where R is the rate of the code. Upon observing the output $\mathbf{Y} = \mathbf{y}$ of a channel with channel law $P_{\mathbf{Y}|\mathbf{X}}$, block-wise maximum a-posteriori decoding can be formulated as the following optimization problem:

$$\begin{aligned}\hat{\mathbf{x}}(\mathbf{y}) &= \arg\max_{\mathbf{x} \in \mathbb{F}_2^n} \; P_{\mathbf{X},\mathbf{Y}}(\mathbf{x}, \mathbf{y}) \\ &= \arg\min_{\mathbf{x} \in \mathbb{F}_2^n} \; -\log P_{\mathbf{X},\mathbf{Y}}(\mathbf{x}, \mathbf{y}),\end{aligned}$$

where $P_{\mathbf{X},\mathbf{Y}}(\mathbf{x}, \mathbf{y}) = P_\mathbf{X}(\mathbf{x}) \cdot P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y}|\mathbf{x})$ is the joint pmf/pdf of the the coded channel input $\mathbf{X}$ and the channel output $\mathbf{Y}$.

We want to be more specific about the code and the channel now, namely we would like to focus on low-density parity-check (LDPC) codes and memoryless channels. So, let $\mathbb{C}$ be an LDPC code defined by some $m \times n$ parity-check matrix $\mathbf{H} \overset{\triangle}{=} (h_{j,i})$, let $\mathcal{I} \overset{\triangle}{=} \{1, \ldots, n\}$ be the set of codeword indices, $\mathcal{J} \overset{\triangle}{=} \{1, \ldots, m\}$ be the set of check indices, $\mathcal{J}_i \overset{\triangle}{=} \{j \in \mathcal{J} \,|\, h_{j,i} = 1\}$ be the set of check indices that involve the i-th bit and $\mathcal{I}_j \overset{\triangle}{=} \{i \in \mathcal{I} \,|\, h_{j,i} = 1\}$ be the set of bits that are involved in the j-th check. If $\mathbf{x} \in \mathbb{F}_2^n$ and $\mathcal{S} \subseteq \mathcal{I}$, we let $\mathbf{x}_\mathcal{S}$ be the sub-vector of those positions of $\mathbf{x}$ whose indices are elements of $\mathcal{S}$ and we define the function $L_{\mathrm{XOR}}(\mathbf{x}_\mathcal{S})$ to be the neglog indicator function of a simple parity-check code of length $|\mathcal{S}|$, i.e. $L_{\mathrm{XOR}}(\mathbf{x}_\mathcal{S}) = 0$ if the modulo-2 sum of the components of $\mathbf{x}_\mathcal{S}$ is zero and $L_{\mathrm{XOR}}(\mathbf{x}_\mathcal{S}) = +\infty$ otherwise. Then it can easily be seen that the function $L_\mathbf{H} : \mathbb{F}_2^n \to \mathbb{R}_+$ with

$$L_\mathbf{H}(\mathbf{x}) \overset{\triangle}{=} \sum_{j \in \mathcal{J}} L_{\mathrm{XOR}}(\mathbf{x}_{\mathcal{I}_j})$$

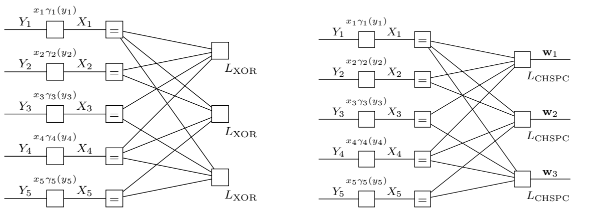

Figure 1: Left: IP-FFG whose global function is f_{IP}; $X_i \in \mathbb{F}_2$. Right: LP-FFG whose global function is f_{LP}; $X_i \in \mathbb{R}$.

is the code neglog indicator function, i.e. it is 0 when $\mathbf{x} \in \mathbb{C}$ and $+\infty$ otherwise and it follows from the last paragraph that the negative logarithm of the pmf $P_{\mathbf{X}}$ can be written as $-\log P_{\mathbf{X}}(\mathbf{x}) = nR\log(2) + L_{\mathbf{H}}(\mathbf{x}) = \mathrm{const} + L_{\mathbf{H}}(\mathbf{x})$. The memoryless assumption about the channel implies $P_{\mathbf{Y}|\mathbf{X}} = \prod_{i\in\mathcal{I}} P_{Y_i|X_i}(y_i|x_i)$ and $-\log P_{\mathbf{X},\mathbf{Y}}(\mathbf{x},\mathbf{y}) = \mathrm{const} + L_{\mathbf{H}}(\mathbf{x}) - \sum_{i\in\mathcal{I}} \log P_{Y_i|X_i}(y_i|x_i)$. Using these results, the maximum a-posteriori decision rule can now be reformulated to read $\hat{\mathbf{x}}(\mathbf{y}) = \arg\min_{\mathbf{x}\in\mathbb{F}_2^n} f_{\mathrm{IP}}(\mathbf{x})$, where

$$f_{\mathrm{IP}}(\mathbf{x}) \stackrel{\triangle}{=} L_{\mathbf{H}}(\mathbf{x}) + \sum_{i\in\mathcal{I}} x_i\gamma_i \tag{1}$$

and $\gamma_i \stackrel{\triangle}{=} \gamma_i(y_i) \stackrel{\triangle}{=} \log(P_{Y_i|X_i}(y_i|0)/P_{Y_i|X_i}(y_i|1))$. The function $f_{\mathrm{IP}}(\mathbf{x})$ can be represented by an FFG: Fig. 1 (left) shows the FFG for an exemplary code $\mathbb{C}$ with $n = 5$ and $m = 3$. An FFG of this type will be called an IP-FFG where IP stands for integer programming.

4. THE LP DECODER

Minimizing $f(\mathbf{x})$ in (1) can be seen as an integer programming problem with a linear cost function. In general, this integer program is computationally intractable because the complexity grows exponentially in the block length n; therefore, block-wise maximum a-posteriori (and also maximum likelihood) decoding of codes is in general computationally infeasible for LDPC codes. Feldman, Karger, and Wainwright [6, 7] proposed to relax this problem in order to obtain a simple LP; the resulting decoder is called the LP decoder. Let us derive the LP decoder in two steps. The first step is to realize that the minimization problem before (1) can be written as[6] $\hat{\mathbf{x}}(\mathbf{y}) = \arg\min_{\mathbf{x}\in\mathbb{R}^n} f(\mathbf{x})$ with

$$f(\mathbf{x}) \stackrel{\triangle}{=} L_{\mathrm{conhull}(\mathbb{C})}(\mathbf{x}) + \sum_{i\in\mathcal{I}} x_i\gamma_i,$$

where $L_{\mathrm{conhull}(\mathbb{C})}(\mathbf{x})$ is the neglog indicator function of the polytope that is the convex hull of $\mathbb{C} \subseteq \mathbb{R}^n$. This minimization problem is equivalent to an LP but the description complexity of the convex hull of $\mathbb{C}$ is exponential in n for general LDPC codes. The second step remedies this problem: instead of minimizing over the convex hull of $\mathbb{C}$ one minimizes over a relaxed region, i.e. a region that can easily be described yet for LDPC codes is not much larger than the convex hull of $\mathbb{C}$. The most canonical relaxation yields[7] $\hat{\mathbf{x}}(\mathbf{y}) = \arg\min_{\mathbf{x}\in\mathbb{R}^n} \min_{\mathbf{w}} f_{\mathrm{LP}}(\mathbf{x},\mathbf{w})$, where $f_{\mathrm{LP}}(\mathbf{x},\mathbf{w}) \stackrel{\triangle}{=} L_{\mathbf{H}}^{\mathrm{rel}}(\mathbf{x},\mathbf{w}) + \sum_{i\in\mathcal{I}} x_i\gamma_i$ with

$$L_{\mathbf{H}}^{\mathrm{rel}}(\mathbf{x},\mathbf{w}) \stackrel{\triangle}{=} \sum_{i\in\mathcal{I}} [\![0 \le x_i \le 1]\!] + \sum_{j\in\mathcal{J}} L_{\mathrm{CHSPC}}(\mathcal{I}_j, \mathbf{x}_{\mathcal{I}_j}, \mathbf{w}_j).$$

The global function $f_{\mathrm{LP}}(\mathbf{x},\mathbf{w})$ is shown by the FFG in Fig. 1 (right); an FFG of this type will be called an LP-FFG. Here, L_{CHSPC} is the neglog indicator function of the convex hull of a simple parity-check code whose length is given by the size of the first argument; it can be written as

$$L_{\mathrm{CHSPC}}(\mathcal{I}_j, \mathbf{x}_{\mathcal{I}_j}, \mathbf{w}_j) \stackrel{\triangle}{=} \left[\!\!\left[\sum_{\mathcal{S}\in\mathcal{E}_j} w_{j,\mathcal{S}} = 1 \right]\!\!\right] + \left(\sum_{\mathcal{S}\in\mathcal{E}_j} [\![w_{j,\mathcal{S}} \ge 0]\!] \right) + \left(\sum_{i\in\mathcal{I}_j} \left[\!\!\left[x_i = \sum_{\mathcal{S}\in\mathcal{E}_j:\ i\in\mathcal{S}} w_{j,\mathcal{S}} \right]\!\!\right] \right),$$

where we have introduced the variables $w_{j,\mathcal{S}}$, $\mathcal{S} \in \mathcal{E}_j$ and the set $\mathcal{E}_j \stackrel{\triangle}{=} \{S \subseteq \mathcal{I}_j : |S| \text{ even}\}$. (E.g. for a check node j involving x_1, x_2, and x_3 we have $\mathcal{E}_j = \{\{\},\{1,2\},\{1,3\},\{2,3\}\}$).

By introducing more/different inequalities one can get other (possibly tighter) relaxations [6]. In this paper we only consider the relaxation presented above, mainly because $L_{\mathbf{H}}^{\mathrm{rel}}(\mathbf{x},\mathbf{w})$ is the neglog indicator function of a polytope that was called the fundamental polytope in [1] (and which characterizes valid configurations of finite covers of Tanner graphs).

5. THE MIN-SUM ALGORITHM DECODER

Let $f : (\mathcal{X}_1 \times \cdots \times \mathcal{X}_n) \to \mathbb{R}$ be the global function of an FFG where the alphabets $\mathcal{X}_i$ can be finite or infinite. The min-sum algorithm (MSA) is a message-passing algorithm that sends messages along edges of an FFG and does some processing at the nodes [8, 3]. If the FFG has no loops then the result is the following: for each i we obtain a function $f_i : \mathcal{X}_i \to \mathbb{R}$ where[8] $f_i(x_i) = \min_{\mathbf{x}:\ \mathbf{x}_{|i}=x_i} f(\mathbf{x})$. If the FFG has loops, then this is in general not the case anymore. Nevertheless, it is well-known that the MSA can be used to decode

[6] This reformulation stems from the fact that if an LP has a unique solution then it must be a vertex of the region one is minimizing over. If there are multiple solutions then at least one vertex is minimal.

[7] The vector $\mathbf{w}$ is an auxiliary vector that helps expressing f_{LP}.

[8] The expression $\mathbf{x}_{|i}$ denotes the i-th component of $\mathbf{x}$.

LDPC codes (whose FFGs in general have loops) and the decoding performance is very good.

Definition 5 (MSA Decoder) *The MSA decoder works as follows: Perform* $\mathrm{MSA}_{\mathrm{IP-FFG}}$*. Because* $\mathcal{X}_i = \mathbb{F}_2$ *we get after* r *iterations for each* $i \in \mathcal{I}$ *some function* $f_i^{\langle r \rangle} : \mathbb{F}_2 \to \mathbb{R}$ *and based on this we can decide* $\hat{x}_i^{\langle r \rangle} = 0$ *if* $f_i^{\langle r \rangle}(0) < f_i^{\langle r \rangle}(1)$ *and* $\hat{x}_i^{\langle r \rangle} = 1$ *otherwise.*

The question we would like to address here is: is there some connection between the result of the MSA decoder and the result of the LP decoder from Sec. 4? A first observation is stated in the next theorem.

Theorem 6 *Performing* $\mathrm{MSA}_{\mathrm{IP-FFG}}$ *gives essentially the same result as performing* $\mathrm{MSA}_{\mathrm{LP-FFG}}$*. More precisely, if* $\mathrm{MSA}_{\mathrm{IP-FFG}}$ *produces the function* ${f_{\mathrm{IP}}}_i^{\langle r \rangle} : \mathbb{F}_2 \to \mathbb{R}$ *after* r *iterations and* $\mathrm{MSA}_{\mathrm{LP-FFG}}$ *produces the function* ${f_{\mathrm{LP}}}_i^{\langle r \rangle} : \mathbb{R} \to \mathbb{R}$ *after* r *iterations, then*

$$
{f_{\mathrm{LP}}}_i^{\langle r \rangle}(x_i) = \begin{cases} (1-x_i){f_{\mathrm{IP}}}_i^{\langle r \rangle}(0) + x_i {f_{\mathrm{IP}}}_i^{\langle r \rangle}(1) & (0 \le x_i \le 1) \\ +\infty & (\textit{otherwise}) \end{cases}
$$

This means that we reach the same decision for $\hat{x}_i^{\langle r \rangle}$*. Moreover, if* $\mathbf{m}^*$ *is a fixed point of the messages of* $\mathrm{MSA}_{\mathrm{LP-FFG}}$ *and* $\mathbf{x}^*$ *is an assignment based on* $\mathbf{m}^*$ *then the components of* $\mathbf{x}^*$ *are either* 0 *or* 1*.*

Proof: (Sketch) One can prove this by comparing the MSA message update rules for both FFGs. □

An important conclusion of Th.6 is that an understanding of $\mathrm{MSA}_{\mathrm{IP-FFG}}$ gives an understanding of $\mathrm{MSA}_{\mathrm{LP-FFG}}$ and vice-versa, however note that by going from the IP to the LP we have changed the setting from a discrete optimization problem to the problem of minimizing a continuous function over a convex set. Another conclusion is that if $\mathbf{x}^*$ is a pseudo-codeword [6, 7, 1] then it must be a codeword.

In a further step, we would like to use Th. 2 in order to characterize the behavior of $\mathrm{MSA}_{\mathrm{IP-FFG}}$ and $\mathrm{MSA}_{\mathrm{LP-FFG}}$, respectively. The main obstactle is that Th. 2 gives in neither case some valuable information. The reason is that the SLT neighborhoods for both FFGs do in general not lead to valid configurations.

Remark 7 *Let* $\mathbb{C}$ *be some LDPC code defined by a parity-check matrix* $\mathbf{H}$*. Let* $\mathbf{m}^*$ *be a fixed point of* $\mathrm{MSA}_{\mathrm{IP-FFG}}$ *and let* $\mathbf{x}^*$ *be the assignment based on* $\mathbf{m}^*$*.*[9] *Let* $\mathbf{x}^*$ *be a valid configuration: in general Th. 2 does* not *imply global minimality of* $\mathbf{x}^*$*.*

Now, let $\mathbf{m}^*$ *be a fixed point of* $\mathrm{MSA}_{\mathrm{LP-FFG}}$ *and let* $(\mathbf{x}^*, \mathbf{w}^*)$ *be the assignment based on* $\mathbf{m}^*$*. Let* $(\mathbf{x}^*, \mathbf{w}^*)$ *be a valid configuration: as in the first case, in general Th. 2 does* not *imply global minimality of* $(\mathbf{x}^*, \mathbf{w}^*)$*.*

Proof: (Sketch) Consider the first statement and let $\mathbf{x}^*$ be a valid configuration. For proving some global minimality result we would like to combine Th. 2 with Rem. 4, but this is not possible as we now explain.

The problem is that points in an SLT neighborhood of $\mathbf{x}^*$ lie outside the set of feasible points, i.e. for LDPC codes where the bit nodes are only connected to more than two check nodes one usually has to change more bits than allowed by an SLT neighborhood in order to obtain a valid configuration. So, when applying Th. 2 we get that $f(\mathbf{x}^*|\mathbf{y}) < f(\mathbf{x}|\mathbf{y})$ for all $\mathbf{x} \neq \mathbf{x}^*$ in the SLT neighborhood of $\mathbf{x}^*$, but this is trivial because usually $f(\mathbf{x}|\mathbf{y}) = +\infty$ for all $\mathbf{x} \neq \mathbf{x}^*$ in the SLT neighborhood of $\mathbf{x}^*$. This result clearly does not give enough information for applying Rem. 4 which requires us to be able to say something about points in the set of all valid configurations. The second statement is proven along the same lines. □

6. THE QP DECODER

In order to avoid problems as encountered in Rem. 7 we propose the following remedy. We introduce a new convex optimization problem (more precisely, a quadratic program (QP)) whose global function is closely related to the global function of the LP. One of the steps in going from the LP to the QP is to replace "hard" equalities by "soft" equalities, i.e. terms like $[\![x = 0]\!]$ in the global function are replaced by terms like $\alpha \cdot x^2$ where $\alpha \gg 1$. The precise statements are given in the next definition, where for every $\varepsilon > 0$ we define a quadratic program $\mathrm{QP}(\varepsilon)$.

Definition 8 *Let* $R_{\mathrm{a},0} > 0$ *and* $R_{\mathrm{b},0} > 0$ *be some constants and let*[10] $R_{\mathrm{a}}(\varepsilon) \triangleq \varepsilon R_{\mathrm{a},0}$ *and* $R_{\mathrm{b}}(\varepsilon) \triangleq R_{\mathrm{b},0}/\varepsilon$ *for some* $\varepsilon > 0$*. We define the global function of the quadratic program* $\mathrm{QP}(\varepsilon)$ *to be*

$$
\begin{aligned}
f_{\mathrm{QP}(\varepsilon)}(\mathbf{x}, \mathbf{w}, \mathbf{g}) \triangleq{} & \sum_{i \in \mathcal{I}} [\![0 \le x_i \le 1]\!] + \sum_{j \in \mathcal{J}} L'_{\mathrm{CHSPC}}(\mathcal{I}_j, \mathbf{x}_{\mathcal{I}_j}, \mathbf{w}, \mathbf{g}) \\
& + \sum_{i \in \mathcal{I}} \gamma_i x_i + \sum_{i \in \mathcal{I}} \frac{(x_i - \frac{1}{2})^2}{2/R_{\mathrm{a}}(\varepsilon)} + \sum_{i \in \mathcal{I}} \sum_{j \in \mathcal{J}_i} \frac{g_{ij}^2}{2/R_{\mathrm{b}}(\varepsilon)}.
\end{aligned}
$$

with

$$
\begin{aligned}
L'_{\mathrm{CHSPC}}(\mathcal{I}_j, \mathbf{x}_{\mathcal{I}_j}, \mathbf{w}, \mathbf{g}) \triangleq{} & \left[\!\!\left[\sum_{\mathcal{S} \in \mathcal{E}_j} w_{j,\mathcal{S}} = 1 \right]\!\!\right] + \sum_{\mathcal{S} \in \mathcal{E}_j} [\![w_{j,\mathcal{S}} \ge 0]\!] \\
& + \sum_{i \in \mathcal{I}_j} \left[\!\!\left[x_i + g_{ij} = \sum_{\mathcal{S} \in \mathcal{E}_j :\, i \in \mathcal{S}} w_{j,\mathcal{S}} \right]\!\!\right].
\end{aligned}
$$

[9] Note that $\mathbf{x}^*$ can be a valid or invalid configuration.

[10] We have chosen the letter R for the following reason: when associating an electrical network to $\mathrm{QP}(\varepsilon)$ (as will be done in Sec. 7) the values $R_{\mathrm{a}}(\varepsilon)$ and $R_{\mathrm{b}}(\varepsilon)$ correspond to resistor values.

Definition 9 (QP Decoder) *For each $\varepsilon > 0$ and each $0 < \delta < 1/2$ we can now define a QP decoder as follows. Solve the quadratic program* $\mathrm{QP}(\varepsilon)$*, i.e. find* $\tilde{\mathbf{x}} \triangleq \arg\min_{\mathbf{x}} \min_{\mathbf{w},\mathbf{g}} f_{\mathrm{QP}(\varepsilon)}(\mathbf{x}, \mathbf{w}, \mathbf{g})$ *and decide $\hat{x}_i = 0$ if $|\tilde{x}_i - 0| < \delta$, $\hat{x}_i = 1$ if $|\tilde{x}_i - 1| < \delta$, and $\hat{x}_i = ?$ otherwise.*

It is easily possible to draw an FFG for the global function $f_{\mathrm{QP}(\varepsilon)}$, such an FFG will be called a $\mathrm{QP}(\varepsilon)$-FFG. Note that compared to the LP-FFG we did not introduce new cycles.

Theorem 10 *In the limit $\varepsilon \to 0$ the solution of* $\mathrm{QP}(\varepsilon)$ *equals the solution of the LP. Moreover, in the limit $\varepsilon \to 0$ the global function of the* $\mathrm{QP}(\varepsilon)$*-FFG is essentially the same as the LP-FFG.*

Proof: (Sketch) Let $(\hat{\mathbf{x}}, \hat{\mathbf{w}})$ minimize f_{LP} and let $(\tilde{\mathbf{x}}(\varepsilon), \tilde{\mathbf{w}}(\varepsilon), \tilde{\mathbf{g}}(\varepsilon))$ minimize $f_{\mathrm{QP}(\varepsilon)}$. It can easily be seen that $(\hat{\mathbf{x}}, \hat{\mathbf{w}}, \mathbf{g} = \mathbf{0})$ is a feasible point (valid configuration) of $f_{\mathrm{QP}(\varepsilon)}$. Because of the penalty terms $g_{ij}^2/(2/R_{\mathrm{b}}(\varepsilon))$ the length of the difference vector $\mathbf{d}(\varepsilon) \triangleq (\hat{\mathbf{x}}, \hat{\mathbf{w}}, \mathbf{g} = \mathbf{0}) - (\tilde{\mathbf{x}}(\varepsilon), \tilde{\mathbf{w}}(\varepsilon), \tilde{\mathbf{g}}(\varepsilon))$ cannot be too large for small ε. In fact, in the limit $\varepsilon \to 0$ the length of the difference vector goes to zero. □

Theorem 11 *Consider* $\mathrm{MSA}_{\mathrm{QP}(\varepsilon)-\mathrm{FFG}}$ *for $\varepsilon > 0$: if the algorithm converges then it delivers the solution to* $\mathrm{QP}(\varepsilon)$*.*

Proof: (Sketch) The idea of introducing the vectors $\mathbf{g}$ in the $\mathrm{QP}(\varepsilon)$ was to "decouple" the variables $\mathbf{x}$ and $\mathbf{w}$. Let $\mathbf{m}^*$ be a fixed point of $\mathrm{MSA}_{\mathrm{QP}(\varepsilon)-\mathrm{FFG}}$ and let $(\mathbf{x}^*, \mathbf{w}^*, \mathbf{g}^*)$ be the assignment based on $\mathbf{m}^*$. Note that the key difference between $\mathrm{MSA}_{\mathrm{LP}-\mathrm{FFG}}$ and $\mathrm{MSA}_{\mathrm{QP}(\varepsilon)-\mathrm{FFG}}$ is that in the latter case the SLT neighborhoods of $(\mathbf{x}^*, \mathbf{w}^*, \mathbf{g}^*)$ imply minimality of $(\mathbf{x}^*, \mathbf{w}^*, \mathbf{g}^*)$.

If $(\mathbf{x}^*, \mathbf{w}^*, \mathbf{g}^*)$ is not a boundary point of the set of all valid configurations then we can apply Th. 2 right away to reach the conclusion in the theorem statement.

If $(\mathbf{x}^*, \mathbf{w}^*, \mathbf{g}^*)$ is not a boundary point of the set of all valid configurations then we can apply Th. 2 in conjunction with Rem. 4. E.g. fix some $j \in \mathcal{J}$; then a configuration $(\mathbf{x}, \mathbf{w}, \mathbf{g})$ that equals $(\mathbf{x}^*, \mathbf{w}^*, \mathbf{g}^*)$ except for the the values $w_{j,\mathcal{S}}$, $\mathcal{S} \in \mathcal{E}_j$ and where g_{ij}, $i \in \mathcal{I}_j$, are chosen such that $L'_{\mathrm{CHSPC}}(\mathcal{I}_j, \mathbf{x}_{\mathcal{I}_j}, \mathbf{w}, \mathbf{g}) = 0$ is in an SLT neighborhood of $(\mathbf{x}^*, \mathbf{w}^*, \mathbf{g}^*)$ yet it still yields a valid configuration. Or, we can fix some $i \in \mathcal{I}$; then a configuration $(\mathbf{x}, \mathbf{w}, \mathbf{g})$ that equals $(\mathbf{x}^*, \mathbf{w}^*, \mathbf{g}^*)$ except for the the value x_i and where g_{ij}, $j \in \mathcal{J}_i$ is chosen such that $L'_{\mathrm{CHSPC}}(\mathcal{I}_j, \mathbf{x}_{\mathcal{I}_j}, \mathbf{w}, \mathbf{g}) = 0$ for all $j \in \mathcal{J}_i$ is in an SLT neighborhood of $(\mathbf{x}^*, \mathbf{w}^*, \mathbf{g}^*)$ yet it still yields a valid configuration. This allows us to use Rem. 4 and come to the conclusion in the theorem statement. □

Remark 12 *In Th. 6 we saw a tight connection between the behavior of* $\mathrm{MSA}_{\mathrm{IP}-\mathrm{FFG}}$ *and* $\mathrm{MSA}_{\mathrm{LP}-\mathrm{FFG}}$*. There is not anymore such a simple connection between* $\mathrm{MSA}_{\mathrm{IP}-\mathrm{FFG}}$ *and* $\mathrm{MSA}_{\mathrm{QP}(\varepsilon)-\mathrm{FFG}}$*. This is probably the price one has to pay in order to get a statement like in Th. 11.*

Note that also other quadratic programs could have been introduced; potentially also slightly simpler ones. But we conjecture that by introducing $\mathrm{QP}(\varepsilon)$ as done above one might be able to say more than what is proved in Th. 11, e.g. one might be able to say when $\mathrm{MSA}_{\mathrm{QP}(\varepsilon)-\mathrm{FFG}}$ converges.

7. ELECTRICAL NETWORK INTERPRETATION OF THE LP AND QP DECODER

Dennis [9] showed that there is a simple way of associating an electrical network (EN) to a convex optimization problem (especially to linear and quadratic programming problems). Such ENs consist of ideal voltage sources, ideal current sources, (linear and nonlinear) resistors, ideal diodes, and DC-transformers. In Dennis' approach, the currents through certain elements of the EN correspond to the components of the solution vector of the primal optimization problem, whereas the voltages across the same elements yield the components of the solution vector of the dual optimization problem. (Equivalently, one can derive an EN where one can also associate the voltages with the solution of the primal problem and the currents with the solution of the dual problem.) In [10, 11] Vontobel and Loeliger explored the connection between FFGs (which represent global functions whose negative exponent is a convex function) and ENs (that are obtained by Dennis' approach). One can show that there is a topographical one-to-one correspondence between the FFG and the EN obtained by Dennis' approach. Various results can be derived, one of them is that the MSA/MPA can be given an interpretation as simplifying an electrical network (for details, see [10, 11]). In a forthcoming paper we will discuss how one can derive the EN that represents f_{LP} and $f_{\mathrm{QP}(\varepsilon)}$, respectively, and also discuss connections between the LP and the Bethe free energy associated to the IP-FFG. Similar to the function $f_{\mathrm{QP}(\varepsilon)}$, the Bethe free energy associated to the IP-FFG can be seen as an approximation to the function f_{LP}, but in this case the situation is somewhat "reversed": while for the function $f_{\mathrm{QP}(\varepsilon)}$ one can formulate a theorem like Th. 11 but performing the MSA is computationally demanding (see Rem. 12), for the

Bethe free energy one can in general not formulate a theorem like Th. 11 on the global minimality, but performing the MSA can be done very efficiently (in fact, the resulting algorithm is essentially equivalent to the sum-product algorithm).

8. CONCLUDING REMARKS

Let us summarize the results of this paper. Let $\mathbf{x}^*(\mathrm{IP})$, $\mathbf{x}^*(\mathrm{LP})$, and $\mathbf{x}^*(\mathrm{QP}(\varepsilon))$ be the solution of the IP, the LP, and the QP(ε) associated to the same LDPC code, respectively. If $\mathbf{m}^*(\mathrm{MSA}_{\mathrm{IP-FFG}})$ is a fixed point of $\mathrm{MSA}_{\mathrm{IP-FFG}}$ then we let $\mathbf{x}^*(\mathbf{m}^*(\mathrm{MSA}_{\mathrm{IP-FFG}}))$ be an assignment based on $\mathbf{m}^*(\mathrm{MSA}_{\mathrm{IP-FFG}})$; we introduce similar notation for $\mathrm{MSA}_{\mathrm{LP-FFG}}$ and $\mathrm{MSA}_{\mathrm{QP}(\varepsilon)-\mathrm{FFG}}$. With this notation, Th. 10 says that

$$\lim_{\varepsilon\to 0} \mathbf{x}^*(\mathrm{QP}(\varepsilon)) = \mathbf{x}^*(\mathrm{LP}).$$

And for $\varepsilon > 0$, Th. 11 says that if $\mathrm{MSA}_{\mathrm{QP}(\varepsilon)-\mathrm{FFG}}$ converges then

$$\mathbf{x}^*(\mathbf{m}^*(\mathrm{MSA}_{\mathrm{QP}(\varepsilon)-\mathrm{FFG}})) = \mathbf{x}^*(\mathrm{QP}(\varepsilon)).$$

This can be used to make the following statement.

Theorem 13 *Let $\varepsilon' > 0$ be some small constant and assume that $\mathrm{MSA}_{\mathrm{QP}(\varepsilon)-\mathrm{FFG}}$ converges for all $0 \leq \varepsilon \leq \varepsilon'$ and that*

$$\lim_{\varepsilon\to 0} \mathbf{x}^*(\mathbf{m}^*(\mathrm{MSA}_{\mathrm{QP}(\varepsilon)-\mathrm{FFG}})) = \mathbf{x}^*(\mathbf{m}^*(\mathrm{MSA}_{\lim_{\varepsilon\to 0}\mathrm{QP}(\varepsilon)-\mathrm{FFG}}))$$

holds and represents a codeword. Then

$$\begin{aligned}\mathbf{x}^*(\mathbf{m}^*(\mathrm{MSA}_{\mathrm{IP-FFG}})) &\overset{\text{(a)}}{=} \mathbf{x}^*(\mathbf{m}^*(\mathrm{MSA}_{\mathrm{LP-FFG}})) \\ &\overset{\text{(b)}}{=} \mathbf{x}^*(\mathrm{LP}) \overset{\text{(c)}}{=} \mathbf{x}^*(\mathrm{IP}).\end{aligned}$$

Proof: (Sketch) First, let us observe that

$$\begin{aligned}&\lim_{\varepsilon\to 0} \mathbf{x}^*(\mathbf{m}^*(\mathrm{MSA}_{\mathrm{QP}(\varepsilon)-\mathrm{FFG}})) \\ &\quad\overset{\text{(d)}}{=} \mathbf{x}^*(\mathbf{m}^*(\mathrm{MSA}_{\lim_{\varepsilon\to 0}\mathrm{QP}(\varepsilon)-\mathrm{FFG}})) \\ &\quad\overset{\text{(e)}}{=} \mathbf{x}^*(\mathbf{m}^*(\mathrm{MSA}_{\mathrm{LP-FFG}})). \qquad (2)\end{aligned}$$

Here, step (d) follows from the assumption in the theorem statement and step (e) from the second statement in Th. 10. Now, we see that in step (a) we used Th. 6, in step (b) we used (2) together with Ths. 11 and 10, and in step (c) we used the fact the IP solution equals the LP solution under the above assumptions. □

We would like to conclude the paper with a few remarks.

- It would be interesting to see if one can give statements under what conditions $\mathrm{MSA}_{\mathrm{QP}(\varepsilon)-\mathrm{FFG}}$ converges; from our experience with Gaussian FFGs we suspect that it converges under rather general conditions. The intuition in solving ENs might also help in answering this question.
- The statements in this paper confirm the robustness observed in practice when decoding LDPC codes with the MSA decoder.
- Reinforcing the observations made in [1], we can say that the results in this paper suggest that the decision regions of the LP decoder seem to give a tight characterization of the decoding regions of the MSA decoder. This is interesting because the decoding regions of the LP decoder have a relatively simple mathematical characterization.

References

[1] R. Koetter and P. O. Vontobel, "Graph covers and iterative decoding of finite-length codes," in *Proc. 3rd Intern. Conf. on Turbo Codes and Related Topics*, (Brest, France), pp. 75–82, Sept. 1–5 2003. Available online under `http://www.ifp.uiuc.edu/~vontobel`.

[2] Y. Weiss and W. T. Freeman, "On the optimality of the max-product belief propagation algorithm in arbitrary graphs," *IEEE Trans. on Inform. Theory*, vol. IT–47, no. 2, pp. 736–744, 2001.

[3] F. R. Kschischang, B. J. Frey, and H.-A. Loeliger, "Factor graphs and the sum-product algorithm," *IEEE Trans. on Inform. Theory*, vol. IT–47, no. 2, pp. 498–519, 2001.

[4] G. D. Forney, Jr., "Codes on graphs: normal realizations," *IEEE Trans. on Inform. Theory*, vol. 47, no. 2, pp. 520–548, 2001.

[5] H.-A. Loeliger, "An introduction to factor graphs," *IEEE Sig. Proc. Mag.*, vol. 21, no. 1, pp. 28–41, 2004.

[6] J. Feldman, *Decoding Error-Correcting Codes via Linear Programming*. PhD thesis, Massachusetts Institute of Technology, Cambridge, MA, 2003. Available online under `http://www.columbia.edu/~jf2189/pubs.html`.

[7] J. Feldman, D. R. Karger, and M. J. Wainwright, "Using linear programming to decode linear codes," in *Proc. 37th annual Conference on Information Sciences and Systems (CISS '03)*, (Baltimore, MD), Mar. 12-14 2003. Available online under `http://www.columbia.edu/~jf2189/pubs.html`.

[8] N. Wiberg, *Codes and Decoding on General Graphs*. PhD thesis, Linköping University, Sweden, 1996.

[9] J. B. Dennis, *Mathematical Programming and Electrical Networks*. The Technology Press of The Massachusetts Institute of Technology, Cambridge, Mass., 1959.

[10] P. O. Vontobel and H.-A. Loeliger, "On factor graphs and electrical networks," in *Mathematical Systems Theory in Biology, Communication, Computation, and Finance, IMA Volumes in Math. & Appl.* (D. Gilliam and J. Rosenthal, eds.), Springer Verlag, 2003.

[11] P. O. Vontobel, *Kalman Filters, Factor Graphs, and Electrical Networks*. Post-Diploma Project, ETH Zurich, 2002. Available online under `http://www.isi.ee.ethz.ch/publications`.