

# Correcting a Fraction of Errors in Nonbinary Expander Codes with Linear Programming

Vitaly Skachek, *Member, IEEE*

**Abstract**—A linear-programming decoder for *nonbinary* expander codes is presented. It is shown that the proposed decoder has the nearest-neighbor certificate properties. It is also shown that this decoder corrects any pattern of errors of a relative weight up to approximately  $\frac{1}{4}\delta_A\delta_B$  (where  $\delta_A$  and  $\delta_B$  are the relative minimum distances of the constituent codes).

**Index Terms**—Expander Codes, Low-Density Parity-Check Codes, Linear-Programming Decoding, Nonbinary Codes.

## I. INTRODUCTION

Low-density parity check (LDPC) codes have become very popular in recent years due to their excellent performance under message-passing (MP) decoders. Yet, our understanding of LDPC codes and their decoders is still limited. While most of the research to date was devoted to binary LDPC codes, there are works suggesting that nonbinary LDPC codes combined with high-order modulation schemes can possibly outperform their binary counterparts (at a price of higher decoding complexity) [12], [18].

For a binary case, a new approach toward understanding of LDPC codes was suggested in [4] and [7]: it was proposed to decode binary LDPC codes using linear-programming (LP) decoder, and important connections between the linear-programming decoding and the message-passing decoding were established (see also [11], [20]). In particular, it was shown that

This work was supported in part by the Claude Shannon Institute for Discrete Mathematics, Coding and Cryptography (Science Foundation Ireland Grant 06/MI/006), and in part by the National Research Foundation of Singapore (Research Grant NRF-CRP2-2007-03). Part of this work was presented at *IEEE International Symposium on Information Theory 2009*, Seoul, Korea.

V. Skachek was with the Claude Shannon Institute and the School of Mathematical Sciences, University College Dublin, Belfield, Dublin 4, Ireland. He is now with the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link, Singapore 637371, e-mail: Vitaly.Skachek@ntu.edu.sg.

the events of LP decoder failures are caused by so-called *pseudocodewords*, and those pseudocodewords are, in turn, related to the failure events of the message-passing decoders.

These results were generalized in [9], [10] toward nonbinary LDPC codes and coded modulations, and in particular to codes over finite quasi-Frobenius rings (see also [8]). It was shown that the connections between LP decoding and MP decoding are preserved in the nonbinary settings as well.

A promising approach for constructing LDPC codes using graphs goes back to [19]. The construction was modified in [17], where *expander graph* was used as an ingredient in a construction of linear-time decodable codes that correct a constant fraction of errors under a variation of an MP decoder. This result was improved in the works [2], [3], [15], [16], [21]. It was shown in [1] that expander codes achieve capacity of a binary symmetric channel under a variation of MP decoder. Explicit constructions of regular expander graphs can be found, for instance, in [13], [14].

In [5], the performance of expander codes in [17] under the LP decoding was investigated. It was shown, that the LP decoder corrects a similar fraction of errors as the MP decoder in [17] does. This research direction was extended in [6], where it was shown that the expander codes achieve the capacity of a variety of binary memoryless channels. It was also shown in [6], that the LP decoder applied to the codes in [21] corrects a similar fraction of errors as the decoder therein, which is approximately a quarter of the lower bound on their relative minimum distance.

In this work, we generalize several results in [6] toward *nonbinary* settings. There are some additional differences between [6] and our work. First, we use a slightly different definition of a (bipartite) expander graph and corresponding code. Second, the analysis in [6] assumes that the all-zero codeword was transmitted, while we do not make such an assumption.

Finally, we present a more accurate analysis of the correctable fraction of errors, and, in particular, we elaborate on the  $o(1)$ -term in the bound on a fraction of correctable errors.

The manuscript is structured as follows. In Section II, we redefine (nonbinary) expander codes. In Section III we define a linear-programming decoder for these codes and discuss some of its basic properties. In Section IV, we present the dual problem and discuss the criteria for the decoding success. In Section V, we present a feasible solution to the dual problem and show that the LP decoder corrects a constant fraction of errors. In Section VI, we present a concept of error pattern orientation. By using this concept, we show that the LP decoder corrects even higher fraction of errors. Finally, in Section VII, we summarize the results presented in this paper and compare them with some known works.

## II. CODE CONSTRUCTION

Below, we revisit the construction in [1].

Let  $\mathcal{G} = (A \cup B, E)$  be a bipartite  $\Delta$ -regular undirected connected graph with a vertex set  $V = A \cup B$  such that  $A \cap B = \emptyset$ , and an edge set  $E$  such that every edge has one endpoint in  $A$  and one endpoint in  $B$ . We denote  $|A| = |B| = n$  and thus  $|E| = \Delta n$ . We assume an ordering on  $V$ , thereby inducing an ordering on  $E = \{e_i\}_{i=1}^{|E|}$ . Let  $\mathbb{F}$  be the field  $\mathbb{F}_q$ . For every vertex  $v \in V$ , we denote by  $E(v)$  the set of edges that are incident with  $v$ . For a word  $\mathbf{z} = (z_e)_{e \in E}$  (whose entries are indexed by  $E$ ) in  $\mathbb{F}^{|E|}$ , we denote by  $(\mathbf{z})_{E(v)}$  the sub-block of  $\mathbf{z}$  that is indexed by  $E(v)$ .

For each  $v \in V$ , let  $\mathcal{C}(v)$  be a linear code of length  $\Delta$  over  $\mathbb{F}$ . The expander code  $\mathbf{C}$  is defined as the following linear code of length  $|E|$  over  $\mathbb{F}$ :

$$\mathbf{C} = \left\{ \mathbf{c} \in \mathbb{F}^{|E|} : (\mathbf{c})_{E(v)} \in \mathcal{C}(v) \text{ for every } v \in V \right\}.$$

Suppose that  $\mathcal{C}_A$  and  $\mathcal{C}_B$  are linear  $[\Delta, r_A \Delta, \delta_A \Delta]$  and  $[\Delta, r_B \Delta, \delta_B \Delta]$  codes over  $\mathbb{F}$ , respectively. In the sequel, we consider the code  $\mathbf{C}$  with

$$\mathcal{C}(v) = \begin{cases} \mathcal{C}_A & \text{for every } v \in A \\ \mathcal{C}_B & \text{for every } v \in B \end{cases}.$$

This code was first studied in [1]. In particular, it was shown therein that the rate of  $\mathbf{C}$  is at least  $r_A + r_B - 1$ .

Denote by  $A_{\mathcal{G}}$  the adjacency matrix of  $\mathcal{G}$ ; namely,  $A_{\mathcal{G}}$  is a  $|V| \times |V|$  real symmetric matrix whose rows and columns are indexed by the set  $V$ , and for every  $u, v \in V$ , the entry in  $A_{\mathcal{G}}$  that is indexed by  $(u, v)$  is given by

$$(A_{\mathcal{G}})_{u,v} = \begin{cases} 1 & \text{if } \{u, v\} \in E \\ 0 & \text{otherwise} \end{cases}.$$

It is known that  $\Delta$  is the largest eigenvalue of  $A_{\mathcal{G}}$ . We denote by  $\gamma_{\mathcal{G}}$  the ratio between the second largest eigenvalue of  $A_{\mathcal{G}}$  and  $\Delta$ . The constructions of  $\Delta$ -regular bipartite expander graphs in [13], [14] have  $\gamma_{\mathcal{G}} \leq 2\sqrt{\Delta - 1}/\Delta$ .

The relative minimum distance of  $\mathbf{C}$ ,  $\delta_{\mathbf{C}}$ , was shown in [15] to satisfy

$$\delta_{\mathbf{C}} \geq \frac{\delta_A \delta_B - \gamma_{\mathcal{G}} \sqrt{\delta_A \delta_B}}{1 - \gamma_{\mathcal{G}}}. \quad (1)$$

In the sequel, we use the notation  $d(\mathbf{x}, \mathbf{z})$  to denote the Hamming distance between the vectors  $\mathbf{x}$  and  $\mathbf{z}$ .

## III. LINEAR-PROGRAMMING DECODER

In this section, we introduce an LP decoder for the code  $\mathbf{C}$ . Suppose that the codeword  $\mathbf{c} = (c_e)_{e \in E} \in \mathbf{C}$  is transmitted through the adversarial channel and the word  $\mathbf{y} = (y_e)_{e \in E} \in \mathbb{F}^{|E|}$  is received.

We define the mapping

$$\xi : \mathbb{F} \longrightarrow \{0, 1\}^q \subset \mathbb{R}^q,$$

by

$$\xi(\beta) = \mathbf{x} = (x^{(\alpha)})_{\alpha \in \mathbb{F}},$$

such that, for each  $\alpha \in \mathbb{F}$ ,

$$x^{(\alpha)} = \begin{cases} 1 & \text{if } \alpha = \beta \\ 0 & \text{otherwise.} \end{cases}$$

The mapping  $\xi$  is one-to-one, and its image is the set of binary vectors of length  $q$  with Hamming weight 1. Please note that this mapping is slightly different from its counterpart in [9], where the image of the mapping was the set of binary vectors of length  $q - 1$  of Hamming weight 0 or 1.

We also define

$$\Xi : \mathbb{F}^{|E|} \longrightarrow \{0, 1\}^{q|E|} \subset \mathbb{R}^{q|E|},$$

according to

$$\Xi(\mathbf{c}) = (\xi(c_{e_1}) \mid \xi(c_{e_2}) \mid \cdots \mid \xi(c_{e_{|E|}})).$$

We note that  $\Xi$  is also one-to-one.

For vectors  $\mathbf{f} \in \mathbb{R}^{q|E|}$ , we adopt the notation

$$\mathbf{f} = (\mathbf{f}_{e_1} \mid \mathbf{f}_{e_2} \mid \cdots \mid \mathbf{f}_{e_{|E|}}),$$

where

$$\forall e \in E, \mathbf{f}_e = (f_e^{(\alpha)})_{\alpha \in \mathbb{F}}.$$

We can write the inverse of  $\Xi$  as

$$\Xi^{-1}(\mathbf{f}) = (\xi^{-1}(\mathbf{f}_{e_1}), \xi^{-1}(\mathbf{f}_{e_2}), \dots, \xi^{-1}(\mathbf{f}_{e_{|E|}})).$$

Below, we define the variables that will be used in the decoder. For all  $e \in E$ ,  $\alpha \in \mathbb{F}$ , we use the variables  $f_e^{(\alpha)} \geq 0$ . The objective function is  $\sum_{e \in E} \sum_{\alpha \in \mathbb{F}} \gamma_e^{(\alpha)} f_e^{(\alpha)}$ , where  $\gamma_e^{(\alpha)}$  is a function of the channel output.

For each  $\alpha \in \mathbb{F}$  we set

$$\gamma_e^{(\alpha)} = \begin{cases} -1 & \text{if } \alpha = y_e \\ 1 & \text{if } \alpha \neq y_e \end{cases}.$$

Assume that  $\mathbf{f}_e = \xi(\beta)$  for some  $e \in E$ ,  $\beta \in \mathbb{F}$ . Then, it is straightforward to verify that

$$\sum_{\alpha \in \mathbb{F}} \gamma_e^{(\alpha)} f_e^{(\alpha)} = \begin{cases} -1 & \text{if } \beta = y_e \\ 1 & \text{if } \beta \neq y_e \end{cases}.$$

Suppose now that  $\mathbf{f} = \Xi(\mathbf{z})$  for some  $\mathbf{z} \in \mathbb{F}^{|E|}$ . It follows that

$$\sum_{e \in E} \sum_{\alpha \in \mathbb{F}} \gamma_e^{(\alpha)} f_e^{(\alpha)} + |E| = 2d(\mathbf{y}, \mathbf{z}). \quad (2)$$

(Recall that the notation  $d(\mathbf{y}, \mathbf{z})$  is used for the Hamming distance between  $\mathbf{y}$  and  $\mathbf{z}$ .) Therefore, finding  $\mathbf{z} \in \mathcal{C}$  such that  $\mathbf{f} = \Xi(\mathbf{z})$  minimizes the left-hand side of (2) is equivalent to the nearest-neighbor decoding of  $\mathbf{y}$ . Instead, however, we will equivalently maximize

$$- \sum_{e \in E} \sum_{\alpha \in \mathbb{F}} \gamma_e^{(\alpha)} f_e^{(\alpha)}. \quad (3)$$

In the sequel, we use the variables  $w_{v,\mathbf{b}}$  for all  $v \in V$  and all  $\mathbf{b} \in \mathcal{C}(v)$ . These variables can be viewed as *relative weights* of local codewords  $\mathbf{b}$  associated with the edges incident with the vertex  $v$ . The corresponding linear-programming problem is presented in Figure 1.

Constraints (5)-(9) form a polytope which we denote by  $\mathcal{Q}$ . In particular, it follows from constraints (5)-(9) that

$$\forall e \in E : \sum_{\alpha \in \mathbb{F}} f_e^{(\alpha)} = 1. \quad (10)$$

Next, we define the decoding algorithm for the code  $\mathcal{C}$ . The decoder optimizes the objective function (4) subject to constraints (5)-(9). If the result  $\mathbf{f}$  is in  $\{0, 1\}^{q|E|}$ , then the decoder outputs  $\Xi^{-1}(\mathbf{f})$  (as it is shown below, this output is then a codeword of  $\mathcal{C}$ ). Otherwise, the decoder declares a *decoding failure*.

We have the following proposition.

*Proposition 3.1:*

- 1) Let  $(\mathbf{f}, \mathbf{w}) \in \mathcal{Q}$  and  $\mathbf{f} \in \{0, 1\}^{q|E|}$ . Then
 
$$\Xi^{-1}(\mathbf{f}) \in \mathcal{C}.$$
- 2) If  $\mathbf{c} \in \mathcal{C}$  then there exists  $\mathbf{w}$  such that  $(\mathbf{f}, \mathbf{w}) \in \mathcal{Q}$  and  $\mathbf{f} = \Xi(\mathbf{c}) \in \{0, 1\}^{q|E|}$ .

*Proof:*

- 1) Suppose  $(\mathbf{f}, \mathbf{w}) \in \mathcal{Q}$  and  $\mathbf{f} \in \{0, 1\}^{q|E|}$ . Let  $\mathbf{c} = \Xi^{-1}(\mathbf{f})$ . By (10),  $\mathbf{c}$  is well defined. Next, fix some  $v \in V$  and let  $\mathbf{a} = (\mathbf{c})_{E(v)}$  (for  $\mathbf{a} = (a_e)_{e \in E(v)}$ ). It follows that for any  $e \in E(v)$ ,  $\alpha \in \mathbb{F}$ ,  $f_e^{(\alpha)} = 1$  if and only if  $a_e = \alpha$ . Let  $\mathbf{d} \in \mathcal{C}(v)$ ,  $\mathbf{d} \neq \mathbf{a}$ . Since  $\mathbf{a}$  and  $\mathbf{d}$  are different, there exists  $\beta \in \mathbb{F}$  and  $e' \in E(v)$  such that  $a_{e'} \neq \beta$  and  $d_{e'} = \beta$ . Then, it follows from (10) and either from (6) or from (7) that

$$0 = f_{e'}^{(\beta)} = \sum_{\mathbf{b} \in \mathcal{C}(v) : b_{e'} = \beta} w_{v,\mathbf{b}},$$

and therefore  $w_{v,\mathbf{d}} = 0$ .

It follows that  $w_{v,\mathbf{d}} = 0$  for all  $\mathbf{d} \in \mathcal{C}(v)$ ,  $\mathbf{d} \neq \mathbf{a}$ , and that  $w_{v,\mathbf{a}} = 1$ . Applying this argument for every  $v \in V$  implies  $\mathbf{c} \in \mathcal{C}$ .

- 2) Assume that  $\mathbf{c} \in \mathcal{C}$ . Let  $\mathbf{f} = \Xi(\mathbf{c})$ . For each  $v \in V$ , we set

$$w_{v,\mathbf{b}} = \begin{cases} 1 & \text{if } \mathbf{b} = (\mathbf{c})_{E(v)} \\ 0 & \text{otherwise} \end{cases}.$$

The reader can easily verify that  $\mathbf{f} \in \{0, 1\}^{q|E|}$  and the corresponding  $(\mathbf{f}, \mathbf{w})$  is in  $\mathcal{Q}$ . ■

The following theorem is an equivalent of the *nearest-neighbor certificate*.

*Theorem 3.2:* Suppose that the LP solver applied to the LP problem in Figure 1 outputs a codeword  $\mathbf{c} \in \mathcal{C}$ . Then,  $\mathbf{c}$  is the nearest-neighbor codeword.

The proof follows from the previous proposition and (2).

---


$$\begin{aligned}
\text{Maximize} \quad & \sum_{e \in E, \alpha \in \mathbb{F}} \left( -\gamma_e^{(\alpha)} \right) \cdot f_e^{(\alpha)} & (4) \\
\text{subject to} \quad & \forall v \in V : \sum_{\mathbf{b} \in \mathcal{C}(v)} w_{v, \mathbf{b}} = 1 ; & (5) \\
\forall e = \{v, u\} \in E, \forall \alpha \in \mathbb{F} : & f_e^{(\alpha)} = \sum_{\mathbf{b} \in \mathcal{C}(v) : b_e = \alpha} w_{v, \mathbf{b}} , & (6) \\
& f_e^{(\alpha)} = \sum_{\mathbf{b} \in \mathcal{C}(u) : b_e = \alpha} w_{u, \mathbf{b}} ; & (7) \\
\forall e \in E, \alpha \in \mathbb{F} : & f_e^{(\alpha)} \geq 0 ; & (8) \\
\forall v \in V, \mathbf{b} \in \mathcal{C}(v) : & w_{v, \mathbf{b}} \geq 0 . & (9)
\end{aligned}$$


---

Fig. 1. Primal LP problem

#### IV. DUAL WITNESS AND UNIQUE SOLUTION

We aim to show that the decoder succeeds given that the number of adversarial errors is bounded from above by a certain constant. We use the *dual witness* approach proposed in [5]. This technique was extended in [6] toward binary expander code. We further extend this technique toward nonbinary settings.

Recall that the codeword  $\mathbf{c} \in \mathcal{C}$  was transmitted. If that is the case, the decoder succeeds if it outputs the same  $\mathbf{c}$ . It follows from Proposition 3.1 that there is only one feasible combination of values of the variables  $w_{v, \mathbf{b}}$  that corresponds to the codeword  $\mathbf{c}$ , namely

$$\forall v \in V : w_{v, \mathbf{b}} = \begin{cases} 1 & \text{if } \mathbf{b} = (\mathbf{c})_{E(v)} \\ 0 & \text{otherwise} \end{cases} .$$

The sufficient criteria for the decoder success is that this solution is the *unique* optimum of the LP decoding problem in Figure 1.

To prove the optimality, we show the existence of a dual feasible solution, such that the value of the objective function of the dual problem is equal to the value of the objective functions of the primal problem. The dual LP problem makes use of the following variables. For each  $\alpha \in \mathbb{F}$ ,  $e \in E$ , and  $v \in V$ , such that  $v$  is an endpoint of  $e$ , there is a variable  $\tau_{v, e}^{(\alpha)}$ . In addition, for each  $v \in V$ , there is a variable  $\sigma_v$ .

The dual LP problem is presented in Figure 2. We set the objective value to be  $|E| - 2d(\mathbf{y}, \mathbf{c})$ , which is the value in (3) under the substitution  $\mathbf{z} = \mathbf{c}$  (this fact easily follows from (2)). This can be achieved by setting, for all  $v \in V$ ,  $\sigma_v = \frac{1}{2}\Delta - d((\mathbf{y})_{E(v)}, (\mathbf{c})_{E(v)})$ .

In order to show the uniqueness of the solution, we slightly modify the dual LP problem. More specifically, we enforce strict inequalities in (12), such that the corresponding dual polytope (denoted by  $\mathcal{P}$ ) becomes as in Figure 3. Generally speaking, the polytope  $\mathcal{P}$  can be unbounded, and thus, sometimes we use the term “open polytope”.

The uniqueness of the solution for the primal LP problem now follows from the following proposition.

*Proposition 4.1:* If there is a feasible point in the polytope  $\mathcal{P}$ , then there is a *unique* optimum for the primal LP problem in Figure 1.

*Proof:* First, it is straight-forward to see that any feasible point  $\boldsymbol{\tau} = \{\tau_{v, e}^{(\alpha)}\}_{v \in V, e \in E, \alpha \in \mathbb{F}}$  in  $\mathcal{P}$  is also a feasible point in the polytope in Figure 2 with  $\sigma_v = \frac{1}{2}\Delta - d((\mathbf{y})_{E(v)}, (\mathbf{c})_{E(v)})$ , for all  $v \in V$ . Then, it follows from (2) that  $(\mathbf{f}, \mathbf{w})$  is an optimal solution for the primal problem in Figure 1, where

$$\forall e \in E : \mathbf{f}_e = \xi(c_e) .$$

Assume that  $(\mathbf{h}, \mathbf{s})$  is another optimal solution for the LP problem in Figure 1.

Inequality (14) implies that

$$\tau_{v, e}^{(\alpha)} + \tau_{u, e}^{(\alpha)} \leq \gamma_e^{(\alpha)} - \varepsilon ,$$

for some small  $\varepsilon > 0$ , for all  $e = \{v, u\} \in E$ ,  $\alpha \in \mathbb{F} \setminus \{c_e\}$ . We define a new cost function  $\hat{\gamma} = \{\hat{\gamma}_e^{(\alpha)}\}_{e \in E, \alpha \in \mathbb{F}}$  for the problem in Figure 1 as follows:

$$\hat{\gamma}_e^{(\alpha)} = \begin{cases} \gamma_e^{(\alpha)} - \varepsilon & \text{if } f_e^{(\alpha)} = 0 \\ \gamma_e^{(\alpha)} & \text{otherwise} \end{cases} .$$

---


$$\begin{aligned} \text{Minimize} \quad & \sum_{v \in V} \sigma_v & (11) \\ \text{subject to} \quad & \forall e = \{v, u\} \in E, \forall \alpha \in \mathbb{F} : \tau_{v,e}^{(\alpha)} + \tau_{u,e}^{(\alpha)} \leq \gamma_e^{(\alpha)} ; & (12) \\ & \forall v \in V, \forall \mathbf{b} \in \mathcal{C}(v) : \sum_{e \in E(v)} \tau_{v,e}^{(b_e)} + \sigma_v \geq 0 . & (13) \end{aligned}$$


---

Fig. 2. Dual LP problem

---


$$\begin{aligned} \forall e = \{v, u\} \in E, \forall \alpha \in \mathbb{F} \setminus \{c_e\} : \tau_{v,e}^{(\alpha)} + \tau_{u,e}^{(\alpha)} < \gamma_e^{(\alpha)} ; & (14) \\ \forall e = \{v, u\} \in E : \tau_{v,e}^{(c_e)} + \tau_{u,e}^{(c_e)} \leq \gamma_e^{(c_e)} ; & (15) \\ \forall v \in V, \forall \mathbf{b} \in \mathcal{C}(v) : \sum_{e \in E(v)} \tau_{v,e}^{(b_e)} \geq -\frac{1}{2}\Delta + d((\mathbf{y})_{E(v)}, (\mathbf{c})_{E(v)}) . & (16) \end{aligned}$$


---

Fig. 3. Dual (open) polytope  $\mathcal{P}$

Observe, that

$$\sum_{e \in E, \alpha \in \mathbb{F}} \left( -\hat{\gamma}_e^{(\alpha)} \right) \cdot f_e^{(\alpha)} = \sum_{e \in E, \alpha \in \mathbb{F}} \left( -\gamma_e^{(\alpha)} \right) \cdot f_e^{(\alpha)} .$$

It follows that  $(\mathbf{f}, \mathbf{w})$  is an optimal solution for the LP problem in Figure 1 under the cost function  $\hat{\gamma}$ .

Note that  $(\mathbf{f}, \mathbf{w})$  corresponds to a codeword  $\mathbf{c}$ , and so its entries are either 0 or 1. Moreover,  $(\mathbf{f}, \mathbf{w}) \neq (\mathbf{h}, \mathbf{s})$ , and so in particular  $\mathbf{f} \neq \mathbf{h}$ . Therefore, there must exist at least one  $e \in E$  such that  $\mathbf{f}_e \neq \mathbf{h}_e$ . For such  $e$ , due to (10) (with respect to  $\mathbf{h}_e$ ), there exists at least one  $\beta \in \mathbb{F}$  such that  $f_e^{(\beta)} = 0$  and  $h_e^{(\beta)} > 0$ . Therefore,

$$\begin{aligned} \sum_{e \in E, \alpha \in \mathbb{F}} \left( -\hat{\gamma}_e^{(\alpha)} \right) \cdot h_e^{(\alpha)} &> \sum_{e \in E, \alpha \in \mathbb{F}} \left( -\gamma_e^{(\alpha)} \right) \cdot h_e^{(\alpha)} \\ &= \sum_{e \in E, \alpha \in \mathbb{F}} \left( -\gamma_e^{(\alpha)} \right) \cdot f_e^{(\alpha)} \\ &= \sum_{e \in E, \alpha \in \mathbb{F}} \left( -\hat{\gamma}_e^{(\alpha)} \right) \cdot f_e^{(\alpha)} , \end{aligned}$$

and this makes a contradiction to the fact that  $(\mathbf{f}, \mathbf{w})$  is an optimal solution to the primal problem under the cost function  $\hat{\gamma}$ . The contradiction follows from the (false) assumption that there is more than one optimal solution for the original primal problem.  $\blacksquare$

The following corollary follows immediately from Proposition 4.1.

*Corollary 4.2:* If there is a feasible point in the polytope  $\mathcal{P}$ , then the decoder in Figure 1 succeeds.

## V. CORRECTING A CONSTANT FRACTION OF ERRORS

Recall that the word  $\mathbf{c} = (c_e)_{e \in E} \in \mathcal{C}$  was transmitted and  $\mathbf{y} = (y_e)_{e \in E} \in \mathbb{F}^{|E|}$  was received. Suppose that  $\mathcal{G} = (A \cup B, E)$  is a  $\Delta$ -regular bipartite graph defined as in Section II.

In this section, we will define a notion of error core. Building on that, we will show that if there is no error core in the graph  $\mathcal{G}$ , then the dual solution can be always found for the appropriate nonbinary LP decoding problem.

*Definition:* The graph  $\mathcal{G}$  has an  $(\zeta_A, \zeta_B)$ -error core (where  $\zeta_A, \zeta_B \in [0, 1]$ ) associated with the word  $\mathbf{y}$  if there exists a subset of edges in error  $E' \subseteq \{e \in E : y_e \neq c_e\}$  and two subsets of vertices  $A' \subseteq A$  and  $B' \subseteq B$  such that  $A' \cup B'$  is the set of all the endpoints of the edges in  $E'$ , and:

- for any  $v \in A'$ :  $|\{E(v) \cap E'\}| \geq \zeta_A \Delta$ ;
- for any  $v \in B'$ :  $|\{E(v) \cap E'\}| \geq \zeta_B \Delta$ .

Below, we inductively define the sets of vertices  $V_i$  (for  $i = 0, 1, \dots, t$ , where  $t$  will be defined later) and the sets of edges  $E_i$  (for  $i = 1, 2, \dots, t$ ) as follows.

- *Basis.* The edge set  $E_1$  will be the set of all edges corresponding to the erroneous symbols in  $\mathbf{y}$ , and the vertex sets  $V_0$  and  $V_1$  will be the endpoints

of edges in  $E_1$ :

$$\begin{aligned} E_1 &= \{e \in E : y_e \neq c_e\}; \\ V_0 &= \{v \in A : E(v) \cap E_1 \neq \emptyset\}; \\ V_1 &= \{v \in B : E(v) \cap E_1 \neq \emptyset\}. \end{aligned}$$

- *Step.* For  $i \geq 2$ :

$$V_i = \left\{ v \in V_{i-2} : \left| \{e \in E(v) \cap E_{i-1}\} \right| \geq \frac{\delta \Delta}{4} \right\},$$

where  $\delta = \delta_A$  if  $i$  is even, and  $\delta = \delta_B$  if  $i$  is odd, and

$$E_i = \left\{ e = \{v, u\} \in E_{i-1} : v \in V_{i-1}, u \in V_i \right\}.$$

*Lemma 5.1:* If  $E_i = \emptyset$  for some finite  $i$ , then the decoder in Figure 1 succeeds.

*Proof:* We show that the decoder succeeds by constructing a feasible point in the polytope  $\mathcal{P}$ . We use  $\epsilon > 0$  to denote the quantity, which can be made as small as desired. The precise value of  $\epsilon$  will be discussed later. We set the variables  $\tau_{u,e}^{(\alpha)}$  as follows.

- Let  $e = \{v, u\} \notin E_1$ . Then, by definition of  $E_1$ ,  $c_e = y_e$ . Assume that  $c_e = \beta$ . We set,  $\tau_{v,e}^{(\beta)} = \tau_{u,e}^{(\beta)} = -1/2$ , and so  $\tau_{v,e}^{(\beta)} + \tau_{u,e}^{(\beta)} \leq \gamma_e^{(\beta)} = -1$ . We also set  $\tau_{v,e}^{(\alpha)} = \tau_{u,e}^{(\alpha)} = 1/2 - \epsilon$  for all  $\alpha \in \mathbb{F} \setminus \{\beta\}$ . In that case,  $\tau_{v,e}^{(\alpha)} + \tau_{u,e}^{(\alpha)} < \gamma_e^{(\alpha)} = 1$ . Therefore, (14) and (15) are satisfied.
- Let  $e = \{v, u\} \in E_1$ . Denote  $c_e = \beta$ . By definition of  $E_1$ ,  $y_e \neq c_e$ . Let  $i^*$  be the value such that  $e \in E_{i^*} \setminus E_{i^*+1}$ . In addition, without loss of generality assume that  $v \in V_{i^*-1}$  and  $u \in V_{i^*}$  (and so  $v \notin V_{i^*+1}$  and  $|E(v) \cap E_{i^*}| < \frac{1}{4}\delta\Delta$ ). Then, we set  $\tau_{v,e}^{(\beta)} = \tau_{u,e}^{(\beta)} = \frac{1}{2}$ . In that case,  $\tau_{v,e}^{(\beta)} + \tau_{u,e}^{(\beta)} \leq \gamma_e^{(\beta)} = 1$ , and so (15) is satisfied. We also set, for all  $\alpha \in \mathbb{F} \setminus \{\beta\}$ ,  $\tau_{v,e}^{(\alpha)} = -\frac{5}{2} - \epsilon$  and  $\tau_{u,e}^{(\alpha)} = \frac{3}{2}$ , which yields  $\tau_{v,e}^{(\alpha)} + \tau_{u,e}^{(\alpha)} < \gamma_e^{(\alpha)} \in \{-1, 1\}$ . Thus, all inequalities (14) are also satisfied.

Table I summarizes the assignments of the values to variables  $\tau_{v,e}^{(\alpha)}$  for all  $e \in E$ ,  $v \in e$  and  $\alpha \in \mathbb{F}$ .

Since  $E_i = \emptyset$  for some finite  $i$  (we set  $t = i + 1$ , where  $i$  is this value), the values of all the variables  $\tau_{v,e}^{(\alpha)}$  are defined. We already showed that all inequalities (14) and (15) are satisfied. Next, we show that inequalities (16) are satisfied. It will be enough to show that for all  $v \in V$ ,  $\mathbf{b} \in \mathcal{C}(v)$ ,

$$\sum_{e \in E(v)} \tau_{v,e}^{(b_e)} \geq -\frac{1}{2}\Delta + d((\mathbf{y})_{E(v)}, (\mathbf{c})_{E(v)}). \quad (17)$$

	$\alpha = c_e$	$\alpha \neq c_e$
$y_e$ is correct	$\tau_{v,e}^{(\alpha)} = -\frac{1}{2}$	$\tau_{v,e}^{(\alpha)} = \frac{1}{2} - \epsilon$
$y_e$ is in error	$\tau_{v,e}^{(\alpha)} = \frac{1}{2}$	$\tau_{v,e}^{(\alpha)} = -\frac{5}{2} - \epsilon$ or $\tau_{v,e}^{(\alpha)} = \frac{3}{2}$ depends on the structure of the error

TABLE I  
ASSIGNMENTS OF THE VALUES TO THE VARIABLES  $\tau_{v,e}^{(\alpha)}$ .

For a vertex  $v \in V$  and a codeword  $\mathbf{b} \in \mathcal{C}(v)$ , we define five sets of indices (edges) as follows:

$$\begin{aligned} \mathcal{E}_1 &= \{e \in E(v) : y_e \text{ is correct and } b_e = c_e\}, \\ \mathcal{E}_2 &= \{e \in E(v) : y_e \text{ is correct and } b_e \neq c_e\}, \\ \mathcal{E}_3 &= \{e \in E(v) : y_e \text{ is in error and } b_e = c_e\}, \\ \mathcal{E}'_4 &= \{e \in E(v) : y_e \text{ is in error,} \\ &\quad b_e \neq c_e \text{ and } \tau_{v,e}^{(b_e)} = -\frac{5}{2} - \epsilon\}, \\ \mathcal{E}''_4 &= \{e \in E(v) : y_e \text{ is in error,} \\ &\quad b_e \neq c_e \text{ and } \tau_{v,e}^{(b_e)} = \frac{3}{2}\}. \end{aligned}$$

(These sets depend on  $v$  and  $\mathbf{b}$ , in addition to their dependence on  $\mathbf{c}$  and  $\mathbf{y}$ . However, we write  $\mathcal{E}_j$  rather than  $\mathcal{E}_j(v, \mathbf{b})$  for the sake of simplicity.)

Then,

$$\begin{aligned} \sum_{e \in E(v)} \tau_{v,e}^{(b_e)} &= \sum_{e \in \mathcal{E}_1} \tau_{v,e}^{(b_e)} + \sum_{e \in \mathcal{E}_2} \tau_{v,e}^{(b_e)} + \sum_{e \in \mathcal{E}_3} \tau_{v,e}^{(b_e)} \\ &\quad + \sum_{e \in \mathcal{E}'_4} \tau_{v,e}^{(b_e)} + \sum_{e \in \mathcal{E}''_4} \tau_{v,e}^{(b_e)} \\ &= \sum_{e \in \mathcal{E}_1} (-\frac{1}{2}) + \sum_{e \in \mathcal{E}_2} (\frac{1}{2} - \epsilon) + \sum_{e \in \mathcal{E}_3} \frac{1}{2} \\ &\quad + \sum_{e \in \mathcal{E}'_4} (-\frac{5}{2} - \epsilon) + \sum_{e \in \mathcal{E}''_4} \frac{3}{2} \\ &\geq \left( -\frac{1}{2}\Delta + d((\mathbf{y})_{E(v)}, (\mathbf{c})_{E(v)}) \right) + \sum_{e \in \mathcal{E}_2} (1 - \epsilon) \\ &\quad + \sum_{e \in \mathcal{E}'_4} (-3 - \epsilon) + \sum_{e \in \mathcal{E}''_4} 1. \end{aligned}$$

In order to prove (17), it will be enough to show that

$$|\mathcal{E}_2| + |\mathcal{E}''_4| \geq 3|\mathcal{E}'_4| + \epsilon(|\mathcal{E}_2| + |\mathcal{E}'_4|). \quad (18)$$

We observe several cases.

- Consider a vertex  $v \in (A \setminus V_0) \cup (B \setminus V_1)$ .  
Then,

$$\left| \{e \in E(v) : y_e \neq c_e\} \right| = |\mathcal{E}_3| + |\mathcal{E}'_4| + |\mathcal{E}''_4| = 0, \quad (19)$$

and so (18) is satisfied for any  $\epsilon \leq 1$ .

- Consider a vertex  $v \in V_0 \cup V_1$ . Let  $\delta = \delta_A$  if  $v \in A$ , and  $\delta = \delta_B$  if  $v \in B$ . Since  $E_i = \emptyset$  for some  $i \in \mathbb{N}$ , we have that  $v \in V_{i^*-1} \setminus V_{i^*+1}$  for some  $i^* \in \mathbb{N}$ . Therefore,

$$|E(v) \cap E_{i^*}| < \frac{1}{4}\delta\Delta.$$

We can write, with respect to this  $v$  and any  $\mathbf{b}$ , that

$$|\mathcal{E}'_4| \leq \frac{1}{4}(\delta - \epsilon')\Delta,$$

or,

$$\delta\Delta \geq 4|\mathcal{E}'_4| + \epsilon'\Delta, \quad (20)$$

for some small  $\epsilon' > 0$ .

- If  $\mathbf{b} = (c)_{E(v)}$ , then obviously  $|\mathcal{E}_2| = |\mathcal{E}'_4| = |\mathcal{E}''_4| = 0$ , and so (18) holds.
- If  $\mathbf{b} \neq (c)_{E(v)}$ , then recall that the relative minimum distance of  $\mathcal{C}(v)$  is at least  $\delta$ . Therefore,  $|\mathcal{E}_2| + |\mathcal{E}'_4| + |\mathcal{E}''_4| \geq \delta\Delta$ , and by using (20):

$$|\mathcal{E}_2| + |\mathcal{E}''_4| \geq \delta\Delta - |\mathcal{E}'_4| \geq 3|\mathcal{E}'_4| + \epsilon'\Delta.$$

We see that (18) holds for all  $\epsilon \leq \epsilon'$ .

We have shown that that in all cases, for sufficiently small  $\epsilon$ , (16) holds, and therefore there exists a feasible point in  $\mathcal{P}$ .  $\blacksquare$

*Lemma 5.2:* If there is no  $(\frac{1}{4}\delta_A, \frac{1}{4}\delta_B)$ -error core, then  $E_i = \emptyset$  for some  $i \in \mathbb{N}$ .

*Proof:* Suppose that there is no  $i \in \mathbb{N}$  such that  $E_i = \emptyset$ . Since for all  $i \in \mathbb{N}$ ,  $E_{i+1} \subseteq E_i$ , we have that there exists some even  $i^* \in \mathbb{N}$ , such that for any  $i \geq i^*$ ,  $E_{i+1} = E_i \neq \emptyset$ . This, in turn, means that  $V_{i^*+2} = V_{i^*}$  and  $V_{i^*+3} = V_{i^*+1}$ . However, this implies (without loss of generality) that every  $v \in V_{i^*+1}$  and  $u \in V_{i^*+2}$  has at least  $\frac{1}{4}\delta_A\Delta$  and  $\frac{1}{4}\delta_B\Delta$  incident edges in  $E_{i^*+1}$ , respectively. It follows that the set of edges  $E_{i^*+1}$  together with the sets  $V_{i^*}$  and  $V_{i^*+1}$  forms a  $(\frac{1}{4}\delta_A, \frac{1}{4}\delta_B)$ -error core.  $\blacksquare$

*Corollary 5.3:* If the LP decoder in Figure 1 fails, then there exists an  $(\frac{1}{4}\delta_A, \frac{1}{4}\delta_B)$ -error core associated with the word  $\mathbf{y}$  in the graph  $\mathcal{G}$ .

The proof follows immediately from Lemmas 5.1 and 5.2.

Next, we show that the LP decoder in Figure 1 corrects all the errors in  $\mathbf{y}$  if the amount of errors in it is at most a fraction of the code length. Consider a subgraph  $\mathcal{H} = (U_A \cup U_B, \mathfrak{E})$  of  $\mathcal{G}$  with  $U_A \subseteq A$ ,  $U_B \subseteq B$  and  $\mathfrak{E} \subseteq E$ . For a vertex  $v \in U_A \cup U_B$  denote by  $\deg_{\mathcal{H}}(v)$  its degree in the graph  $\mathcal{H}$ . We use the following known result.

*Proposition 5.4:* Let  $U_A$  and  $U_B$  be subsets of sizes  $|U_A| = a|A|$  and  $|U_B| = b|B|$ , respectively, such that  $a + b > 0$ . Let  $\mathfrak{E}$  be the edge set induced by the vertex set  $U_A \cup U_B$ , and denote  $\mathcal{H} = (U_A \cup U_B, \mathfrak{E})$ . Then,

$$\begin{aligned} 2|\mathfrak{E}| &= \sum_{v \in U_A \cup U_B} \deg_{\mathcal{H}}(v) \\ &\leq 2 \left( ab + \gamma_{\mathcal{G}} \sqrt{a(1-a)b(1-b)} \right) \Delta n \\ &\leq 2((1 - \gamma_{\mathcal{G}})ab + \gamma_{\mathcal{G}}\sqrt{ab})\Delta n. \end{aligned} \quad (21)$$

This statement is equivalent to Proposition 3.3 in [15]. The first inequality is obtained when the tighter inequality in Lemma 3.2 in [15] is used in the proof of Proposition 3.3. If the graph is a Ramanujan expander as in [13], [14], then for fixed  $a$  and  $b$ , by increasing  $\Delta$  (and so by reducing  $\gamma_{\mathcal{G}}$ ), it is possible to make  $|\mathfrak{E}|/(\Delta n)$  as close to  $(ab)$  as desired.

By using Proposition 5.4, we obtain the following theorem.

*Theorem 5.5:* Assume that the size of error in  $\mathbf{y}$  is less than

$$\frac{\zeta_A \zeta_B - \gamma_{\mathcal{G}} \sqrt{\zeta_A \zeta_B}}{1 - \gamma_{\mathcal{G}}} \cdot \Delta n,$$

for some  $\zeta_A, \zeta_B \in (0, 1]$ , such that  $\gamma_{\mathcal{G}} \leq \sqrt{\zeta_A \zeta_B}$ . Then, the graph  $\mathcal{G}$  contains no  $(\zeta_A, \zeta_B)$ -error core associated with this  $\mathbf{y}$ .

The proof of this theorem is along the same lines as the proof of Theorem 3.1 in [15]. For the sake of completeness of the presentation, we place the sketch of the proof in Appendix.

The main result of this section follows from Corollary 5.3 and Theorem 5.5, and it appears in the following corollary.

*Corollary 5.6:* If the size of error in  $\mathbf{y}$  is less than

$$\frac{\delta_A \delta_B / 16 - \gamma_G \sqrt{\delta_A \delta_B / 16}}{1 - \gamma_G} \cdot \Delta n,$$

and  $\gamma_G \leq \frac{1}{4} \sqrt{\delta_A \delta_B}$ , then the LP decoder in Figure 1 will correct all errors in  $\mathbf{y}$ .

Observe, that the proposed LP decoder corrects any error pattern of size approximately  $\delta_A \delta_B \Delta n / 16$ , when the value of  $\Delta$  is large enough.

## VI. USING ERROR PATTERN ORIENTATION

In this section, we present more powerful decoder analysis than its counterpart in Section V. More specifically, by using *error pattern orientation*, we are able to improve the fraction of correctable errors in Section V by approximately a factor of 4. The idea of using error pattern orientation was proposed in [6].

Let  $\mathcal{G} = (A \cup B, E)$  be a  $\Delta$ -regular bipartite graph as before, and let  $\mathcal{H} = (U_A \cup U_B, \mathfrak{E})$  be a subgraph with  $U_A \subseteq A$ ,  $U_B \subseteq B$  and  $\mathfrak{E} \subseteq E$ . We start with the following definition.

*Definition:* The assignment of the directions to the edges of the subgraph  $\mathcal{H} = (U_A \cup U_B, \mathfrak{E})$  is called an  $(\rho_A, \rho_B)$ -orientation (for some  $\rho_A, \rho_B \in (0, 1]$ ) if each vertex  $v \in U_A$  and each vertex  $v \in U_B$  has at most  $\rho_A \Delta$  and  $\rho_B \Delta$  incoming edges in  $\mathfrak{E}$ , respectively. We will say that for the given assignment of the edge directions,  $M$  edges are *violating the  $(\rho_A, \rho_B)$ -orientation property at the vertex  $v \in U_A$  ( $v \in U_B$ )* if  $v$  has  $\rho_A \Delta + M$  ( $\rho_B \Delta + M$ , respectively) incoming edges in  $\mathfrak{E}$ . We will also say that for the given assignment of the edge directions,  $M$  edges are *violating the  $(\rho_A, \rho_B)$ -orientation property in  $\mathcal{H}$*  if  $M$  is the smallest integer such that by removing  $M$  edges from  $\mathfrak{E}$ , the resulting  $\mathcal{H}$  will have a  $(\rho_A, \rho_B)$ -orientation.

*Lemma 6.1:* Let  $\mathcal{H} = (U_A \cup U_B, \mathfrak{E})$  be a subgraph of  $\mathcal{G} = (A \cup B, E)$  with  $U_A \subseteq A$ ,  $U_B \subseteq B$  and  $\mathfrak{E} \subseteq E$ . Assume that

$$|\mathfrak{E}| \leq \frac{\mu_A \mu_B - \gamma_G \sqrt{\mu_A \mu_B}}{1 - \gamma_G} \cdot \Delta n,$$

for some  $\mu_A, \mu_B \in (0, 1]$ , such that  $\gamma_G \leq \sqrt{\mu_A \mu_B}$ , and  $\frac{1}{2} \mu_A \Delta$ ,  $\frac{1}{2} \mu_B \Delta$  are both integers. Then,  $\mathfrak{E}$  contains an  $(\mu_A/2, \mu_B/2)$ -orientation.

*Proof:* Assign directions to the edges in  $\mathfrak{E}$  such that the number of violations of an  $(\mu_A/2, \mu_B/2)$ -orientation in  $\mathcal{H}$  is minimal. We will show that if for some  $v \in U_A$  ( $v \in U_B$ ) there are more than  $\mu_A \Delta / 2$  ( $\mu_B \Delta / 2$ , respectively) incoming edges, then it is possible to change the directions of the edges in the graph such that the number of edges violating the orientation property will decrease. This will make a contradiction to the minimality of the number of orientation violations in the current assignment of the edge directions.

Denote by  $\deg_{\text{in}}(v)$  the number of incoming edges (in  $\mathcal{H}$ ) of the vertex  $v$ . Recall that  $\mu_A \Delta$  and  $\mu_B \Delta$  are even integers. We will use the following definitions.

*Definition:* A vertex  $v \in U_A \cup U_B$  is called a *heavy* vertex if it satisfies one of the following:

- 1)  $v \in U_A$  and  $\deg_{\text{in}}(v) > \frac{1}{2} \mu_A \Delta$ ;
- 2)  $v \in U_B$  and  $\deg_{\text{in}}(v) > \frac{1}{2} \mu_B \Delta$ .

*Definition:* A vertex  $v \in U_A \cup U_B$  is called a *full* vertex if it satisfies one of the following:

- 1)  $v \in U_A$  and  $\deg_{\text{in}}(v) = \frac{1}{2} \mu_A \Delta$ ;
- 2)  $v \in U_B$  and  $\deg_{\text{in}}(v) = \frac{1}{2} \mu_B \Delta$ .

*Definition:* A vertex  $v \in U_A \cup U_B$  is called a *light* vertex if it satisfies one of the following:

- 1)  $v \in U_A$  and  $\deg_{\text{in}}(v) < \frac{1}{2} \mu_A \Delta$ ;
- 2)  $v \in U_B$  and  $\deg_{\text{in}}(v) < \frac{1}{2} \mu_B \Delta$ .

Observe that the orientation property is not violated at the full and at the light vertices. Assume, by contrary, that there exists a heavy vertex in  $U_A \cup U_B$ . We show that it is possible to change the directions of the edges in  $\mathfrak{E}$  such that the total number of edges violating the orientation property in  $\mathcal{H}$  will decrease.

Define a set of vertices  $U$  to be the maximal set as follows:

- If  $v \in U_A \cup U_B$  is heavy then  $v \in U$ .
- If  $u \in U_A \cup U_B$  is full and there is a direct edge from  $u$  to  $v$  for some  $v \in U$ , then  $u \in U$ .

The set  $U$  is well defined.

If there is an edge  $(w, u)$  for some  $w \notin U$  and  $u \in U$ , then  $w$  is *light* and there exists a path from  $w$  to some *heavy* vertex  $v \in U$  (vertex  $u$  can be full). Then, it is possible to flip the directions of all edges in

the path, and thus to decrease the number of violations of the orientation property by 1 (at the vertex  $v$ ).

Below, we assume that there is no edge  $(w, u)$  for any  $w \notin U$  and  $u \in U$ . Denote  $U'_A = U \cap U_A$  and  $U'_B = U \cap U_B$ . Let  $\mathfrak{E}'$  be a set of edges in  $\mathfrak{E}$  having one endpoint in  $U'_A$  and one endpoint in  $U'_B$ . Let  $a = |U'_A|/n$  and  $b = |U'_B|/n$ . We have

$$\begin{aligned} \frac{1}{2}(a\mu_A + b\mu_B)\Delta n &\leq |\mathfrak{E}'| \leq |\mathfrak{E}| \\ &\leq \frac{\mu_A\mu_B - \gamma\mathcal{G}\sqrt{\mu_A\mu_B}}{1 - \gamma\mathcal{G}} \cdot \Delta n, \end{aligned} \quad (22)$$

where the first inequality is correct since there are only heavy and full vertices in  $U'_A \cup U'_B$ , and at least one of these vertices is heavy. The last inequality is given by the conditions of the lemma.

Assume that the ratio between the number of directed edges in  $\mathfrak{E}'$  from  $U'_A$  to  $U'_B$  and the number of directed edges in  $\mathfrak{E}'$  from  $U'_B$  to  $U'_A$  is  $\kappa > 0$ . Then,

$$\begin{aligned} \frac{1}{2}a\mu_A(1 + \kappa) \cdot \Delta n &\leq |\mathfrak{E}'| \\ &\leq \left( (1 - \gamma\mathcal{G})ab + \gamma\mathcal{G}\sqrt{ab} \right) \Delta n, \end{aligned} \quad (23)$$

and

$$\begin{aligned} \frac{1}{2}b\mu_B(1 + 1/\kappa) \cdot \Delta n &\leq |\mathfrak{E}'| \\ &\leq \left( (1 - \gamma\mathcal{G})ab + \gamma\mathcal{G}\sqrt{ab} \right) \Delta n, \end{aligned} \quad (24)$$

where the left-hand side inequalities follow from the fact that every vertex in  $U'_A$  and every vertex in  $U'_B$  is either full or heavy, and the right-hand side inequalities follow from (21).

Inequalities (23) and (24) yield

$$b \geq \frac{\mu_A(1 + \kappa)}{2(1 - \gamma\mathcal{G})} - \frac{\gamma\mathcal{G}}{1 - \gamma\mathcal{G}} \sqrt{\frac{b}{a}}, \quad (25)$$

and

$$a \geq \frac{\mu_B(1 + 1/\kappa)}{2(1 - \gamma\mathcal{G})} - \frac{\gamma\mathcal{G}}{1 - \gamma\mathcal{G}} \sqrt{\frac{a}{b}}, \quad (26)$$

respectively.

Consider two cases.

Case 1:  $a\mu_A(1 + \kappa) \geq b\mu_B(1 + 1/\kappa)$ . Then, from (25) we have

$$b \geq \frac{\mu_A(1 + \kappa)}{2(1 - \gamma\mathcal{G})} - \frac{\gamma\mathcal{G}}{1 - \gamma\mathcal{G}} \sqrt{\frac{\mu_A(1 + \kappa)}{\mu_B(1 + 1/\kappa)}},$$

and, so,

$$b\mu_B \geq \frac{\mu_A\mu_B(1 + \kappa)}{2(1 - \gamma\mathcal{G})} - \frac{\gamma\mathcal{G}}{1 - \gamma\mathcal{G}} \sqrt{\mu_A\mu_B\kappa}.$$

Finally,

$$\begin{aligned} a\mu_A &\geq b\mu_B \frac{1 + 1/\kappa}{1 + \kappa} \\ &\geq \frac{\mu_A\mu_B(1 + 1/\kappa)}{2(1 - \gamma\mathcal{G})} - \frac{\gamma\mathcal{G}}{1 - \gamma\mathcal{G}} \sqrt{\frac{\mu_A\mu_B}{\kappa}}. \end{aligned}$$

Case 2:  $a\mu_A(1 + \kappa) < b\mu_B(1 + 1/\kappa)$ . Then, from (26) we have

$$a > \frac{\mu_B(1 + 1/\kappa)}{2(1 - \gamma\mathcal{G})} - \frac{\gamma\mathcal{G}}{1 - \gamma\mathcal{G}} \sqrt{\frac{\mu_B(1 + 1/\kappa)}{\mu_A(1 + \kappa)}},$$

and, so,

$$a\mu_A > \frac{\mu_A\mu_B(1 + 1/\kappa)}{2(1 - \gamma\mathcal{G})} - \frac{\gamma\mathcal{G}}{1 - \gamma\mathcal{G}} \sqrt{\frac{\mu_A\mu_B}{\kappa}}.$$

We also obtain:

$$\begin{aligned} b\mu_B &> a\mu_A \frac{1 + \kappa}{1 + 1/\kappa} \\ &> \frac{\mu_A\mu_B(1 + \kappa)}{2(1 - \gamma\mathcal{G})} - \frac{\gamma\mathcal{G}}{1 - \gamma\mathcal{G}} \sqrt{\mu_A\mu_B\kappa}. \end{aligned}$$

From (22), in both cases we have:

$$\begin{aligned} |\mathfrak{E}| &> \frac{1}{2}(a\mu_A + b\mu_B)\Delta n \\ &\geq \frac{1}{2} \left( \frac{\mu_A\mu_B(2 + \kappa + 1/\kappa)}{2(1 - \gamma\mathcal{G})} \right. \\ &\quad \left. - \frac{\gamma\mathcal{G}\sqrt{\mu_A\mu_B}}{1 - \gamma\mathcal{G}} \left( \sqrt{\kappa} + \sqrt{\frac{1}{\kappa}} \right) \right) \Delta n. \end{aligned} \quad (27)$$

Denote

$$\eta = \sqrt{\kappa} + \sqrt{1/\kappa}, \quad \eta \in [2, +\infty).$$

Observe that the right-hand side of (27) is a quadratic function of  $\eta$ . Since  $\gamma\mathcal{G} \leq \sqrt{\mu_A\mu_B}$ , we have that this function is nonnegative and monotonic increasing for  $\eta \geq 2\gamma\mathcal{G}/\sqrt{\mu_A\mu_B}$ . Its minimum is obtained for the smallest value of  $\eta$ , which is achieved at  $\kappa = 1$ . Therefore, (27) becomes

$$|\mathfrak{E}| > \frac{\mu_A\mu_B - \gamma\mathcal{G}\sqrt{\mu_A\mu_B}}{1 - \gamma\mathcal{G}} \cdot \Delta n.$$

We obtained a contradiction to the right-hand side of (22).

The contradiction follows from the assumption that there exists a heavy vertex in  $U_A \cup U_B$ , and it is impossible to flip the directions of the edges such that the

number of violations of the orientation property will decrease. We conclude that there is an  $(\mu_A/2, \mu_B/2)$ -orientation in  $\mathfrak{E}$ .  $\blacksquare$

Define the numbers  $\theta_A$  and  $\theta_B$  as follows. Let  $\theta_A > 0$  ( $\theta_B > 0$ ) be the largest number such that  $\theta_A < \delta_A$  ( $\theta_B < \delta_B$ ) and  $\frac{1}{4}\theta_A\Delta$  ( $\frac{1}{4}\theta_B\Delta$ , respectively) is integer.

The following theorem is the main result of this paper.

*Theorem 6.2:* Let  $C$  be defined as above, and assume that  $\gamma_G \leq \frac{1}{2}\sqrt{\theta_A\theta_B}$ . Then, the decoder in Figure 1 is able to correct any error pattern of a size less than or equal to

$$\frac{\theta_A\theta_B - 2\gamma_G\sqrt{\theta_A\theta_B}}{4(1 - \gamma_G)} \cdot \Delta n$$

in a codeword  $c \in C$ .

*Proof:* Let  $\mathfrak{E}$  be the set of edges in error (for a received word  $\mathbf{y}$ ), and assume that

$$|\mathfrak{E}| \leq \frac{\theta_A\theta_B - 2\gamma_G\sqrt{\theta_A\theta_B}}{4(1 - \gamma_G)} \cdot \Delta n.$$

Then, by Lemma 6.1, there exists an  $(\theta_A/4, \theta_B/4)$ -orientation of  $\mathfrak{E}$ .

Therefore, we are able to construct a feasible solution for the dual LP problem, as follows.

- For the edges  $e \notin \mathfrak{E}$ , we set the values of  $\tau_{v,e}^{(\alpha)}$  in the same way as we set the values of  $\tau_{v,e}^{(\alpha)}$  for  $e \notin E_1$  in the proof of Lemma 5.1.
- For the (directed) edge  $(u, v) \in \mathfrak{E}$ , we set

$$\forall \alpha \in \mathbb{F} \setminus \{c_e\} : \tau_{v,e}^{(\alpha)} = -\frac{5}{2} - \epsilon \text{ and } \tau_{u,e}^{(\alpha)} = \frac{3}{2},$$

and

$$\tau_{u,e}^{(c_e)} = \tau_{v,e}^{(c_e)} = \frac{1}{2}.$$

These settings clearly satisfy all the constraints (14) and (15). Moreover, since for every  $v \in A$  ( $v \in B$ ) there are less than  $\frac{1}{4}\delta_A\Delta$  ( $\frac{1}{4}\delta_B\Delta$ , respectively) incident edges  $e \in \mathfrak{E}$  with the corresponding  $\tau_{v,e}^{(\alpha)} = -\frac{5}{2} - \epsilon$ , using the same argument as in Lemma 5.1, for  $\epsilon$  small enough, we have that (16) is also satisfied.  $\blacksquare$

## VII. DISCUSSION

The relative minimum distance of the code  $C$  was shown in [15] to satisfy (1). By taking a sufficiently

large  $\Delta$ , this bound can be made arbitrarily close to  $\delta_A\delta_B$ . Thus, the analysis in Section V demonstrates that the decoder in Figure 1 is able to correct any error pattern of size approximately  $\frac{1}{16}$  of this lower bound. For comparison, the analysis in Section VI shows that the decoder is actually able to correct approximately four times more errors, than it was shown in Section V. Consequently, the fraction of correctable errors under the decoder in Figure 1 is (at least) approximately  $\frac{1}{4}\delta_A\delta_B$ .

It is interesting to compare this result with other related works. Thus, in [21] the code  $C$  with  $\delta_A = \delta_B = \delta$  (for  $0 < \delta < 1$ ) was considered, and a bit-flipping decoder was presented. This decoder corrects approximately  $\frac{1}{4} \cdot \delta^2$  fraction of errors. Similar result for binary codes was also obtained in [6] by using a *linear-programming* decoder and a slightly different definition of expander graph.

However, the fraction of correctable errors in  $C$  can be boosted close to  $\frac{1}{2}\delta_A\delta_B$  by using more advanced decoding techniques [2], [15], [16]. It is still an open question whether the similar fraction of errors can be corrected by using decoder based on linear-programming methods.

The fraction of correctable errors grows with the size of the alphabet (as well as the relative minimum distance does). For example, consider a binary code  $C$  having the same constituent code  $\mathcal{C} = \mathcal{C}(v)$  for each  $v \in V$ . If  $\mathcal{C}$  is a random code of relative minimum distance  $\delta$  and rate  $r$ , then we have (with high probability)

$$r \geq 1 - h_2(\delta) - o(1),$$

where  $h_2(\cdot)$  is the binary entropy function. The rate of  $C$  is at least  $2r - 1$  and the fraction of the correctable errors is arbitrarily close to  $\frac{1}{4} \cdot \delta^2$ . In Table II, we present the relations between the code rate and the lower bound on the fraction of correctable errors.

Next, consider a code  $C$  over a large alphabet. Take  $\mathcal{C} = \mathcal{C}(v)$  (for each  $v \in V$ ) to be Generalized Reed-Solomon code of relative minimum distance  $\delta$  and rate  $r \geq 1 - \delta$ . In this case, we also have to require that  $q \geq \Delta$ . Table III presents the relations between the rate of such  $C$  and the fraction of correctable errors.

## APPENDIX

*Sketch of the proof of Theorem 5.5.*

Rate of C	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9
Fraction of correctable errors, $\times 10^{-4}$	22.14	15.76	10.82	7.086	4.346	2.422	1.160	0.4217	0.0786

TABLE II  
LOWER BOUND ON THE FRACTION OF CORRECTABLE ERRORS FOR VARIOUS RATES OF C, FOR BINARY ALPHABET.

Rate of C	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9
Fraction of correctable errors, $\times 10^{-2}$	5.0625	4.0	3.0625	2.250	1.5625	1.0	0.5625	0.250	0.0625

TABLE III  
LOWER BOUND ON THE FRACTION OF CORRECTABLE ERRORS FOR VARIOUS RATES OF C, FOR LARGE ALPHABET.

Assume, by contrary, that  $\mathcal{G}$  contains a  $(\zeta_A, \zeta_B)$ -error core associated with  $\mathbf{y}$ . Let  $E' \subseteq E$  be the set of edges in this error core, and  $A' \subseteq A$  and  $B' \subseteq B$  such that  $A' \cup B'$  is the set of all the endpoints of the edges in  $E'$ . We have

- for any  $v \in A'$ :  $|\{E(v) \cap E'\}| \geq \zeta_A \Delta$ ;
- for any  $v \in B'$ :  $|\{E(v) \cap E'\}| \geq \zeta_B \Delta$ .

Consider a subgraph  $\mathcal{H} = (U_A \cup U_B, \mathfrak{E})$  of  $\mathcal{G}$  with  $U_A = A'$ ,  $U_B = B'$  and  $\mathfrak{E} = E'$ . Let  $\mathbf{a} = |U_A|/|A|$  and  $\mathbf{b} = |U_B|/|B|$ . From Proposition 5.4, we have

$$|E'| \leq ((1 - \gamma_{\mathcal{G}})\mathbf{a}\mathbf{b} + \gamma_{\mathcal{G}}\sqrt{\mathbf{a}\mathbf{b}})\Delta n. \quad (28)$$

On the other hand, since  $E'$  is the set of edges of an  $(\zeta_A, \zeta_B)$ -error core, we have

$$|E'| \geq \mathbf{a}n \cdot \zeta_A \Delta \quad \text{and} \quad |E'| \geq \mathbf{b}n \cdot \zeta_B \Delta. \quad (29)$$

There are two possibilities:

Case 1:  $\mathbf{a}\zeta_A \geq \mathbf{b}\zeta_B$ . Then, from (28) and (29), we have

$$\mathbf{a}\zeta_A \leq ((1 - \gamma_{\mathcal{G}})\mathbf{a}\mathbf{b} + \gamma_{\mathcal{G}}\sqrt{\mathbf{a}\mathbf{b}}),$$

and so

$$\mathbf{b} \geq \frac{\zeta_A - \gamma_{\mathcal{G}}\sqrt{\mathbf{b}/\mathbf{a}}}{1 - \gamma_{\mathcal{G}}} \geq \frac{\zeta_A - \gamma_{\mathcal{G}}\sqrt{\zeta_A/\zeta_B}}{1 - \gamma_{\mathcal{G}}}.$$

Case 2:  $\mathbf{a}\zeta_A < \mathbf{b}\zeta_B$ . Then, from (28) and (29), similarly we have

$$\mathbf{a} \geq \frac{\zeta_B - \gamma_{\mathcal{G}}\sqrt{\zeta_B/\zeta_A}}{1 - \gamma_{\mathcal{G}}}.$$

In both cases,

$$|E'| \geq \frac{\zeta_A \zeta_B - \gamma_{\mathcal{G}}\sqrt{\zeta_A \zeta_B}}{1 - \gamma_{\mathcal{G}}} \cdot \Delta n,$$

in contradiction with the assumption. This concludes the proof.

## ACKNOWLEDGMENTS

The author wishes to thank Marcus Greferath.

## REFERENCES

- [1] A. Barg and G. Zémor, "Error exponents of expander codes," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1725–1729, June 2002.
- [2] A. Barg and G. Zémor, "Concatenated codes: serial and parallel," *IEEE Trans. Inf. Theory*, vol. 51, no. 5, pp. 1625–1634, May 2005.
- [3] A. Barg and G. Zémor, "Distance properties of expander codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 1, pp. 78–90, Jan. 2006.
- [4] J. Feldman, *Decoding Error-Correcting Codes via Linear Programming*, Ph.D. Thesis, Massachusetts Institute of Technology, Sep. 2003.
- [5] J. Feldman, T. Malkin, R. Servedio, C. Stein, and M.J. Wainwright, "LP decoding corrects a constant fraction of errors," *IEEE Trans. Inf. Theory*, vol. 53, no. 1, pp. 82–89, Jan. 2007.
- [6] J. Feldman and C. Stein, "LP decoding achieves capacity," in *Proc. ACM-SIAM Symposium on Discrete Algorithms (SODA)*, Vancouver, Canada, Jan. 2005.
- [7] J. Feldman, M.J. Wainwright, and D.R. Karger, "Using linear programming to decode binary linear codes," *IEEE Trans. Inf. Theory*, vol. 51, no. 3, pp. 954–972, Mar. 2005.
- [8] M.F. Flanagan, "Codeword-independent performance of nonbinary linear codes under linear-programming and sum-product decoding," in *Proc. IEEE International Symposium on Information Theory (ISIT)*, Toronto, Canada, July 2008.
- [9] M.F. Flanagan, V. Skachek, E. Byrne, and M. Greferath, "Linear-programming decoding of nonbinary linear codes," in *Proc. 7th International ITG Conference on Source and Channel Coding (SCC)*, Ulm, Germany, Jan. 2008.
- [10] M.F. Flanagan, V. Skachek, E. Byrne, and M. Greferath, "Linear-programming decoding of nonbinary linear codes," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4134–4154, Sep. 2009.
- [11] R. Koetter and P. Vontobel, "Graph-cover decoding and finite-length analysis of message-passing iterative decoding of LDPC codes," to appear in *IEEE Trans. Inf. Theory*. Also available at <http://www.arxiv.org/abs/cs.IT/0512078>.
- [12] X. Li, M.R. Soleymani, J. Lodge, and P.S. Guinand, "Good LDPC codes over  $\text{GF}(q)$  for bandwidth efficient transmission," in *Proc. 4-th IEEE Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, June 2003.
- [13] A. Lubotsky, R. Philips, and P. Sarnak, "Ramanujan graphs," *Combinatorica*, vol. 8, no. 3, pp. 261–277, 1988.

- [14] G.A. Margulis, "Explicit group theoretical constructions of combinatorial schemes and their applications to the design of expanders and concentrators," *Probl. Inform. Transm.*, vol. 24, no. 1, pp. 39–46, 1988.
- [15] R.M. Roth and V. Skachek, "Improved nearly-MDS expander codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 8, pp. 3650–3661, Aug. 2006.
- [16] V. Skachek and R.M. Roth, "Generalized minimum distance iterative decoding of expander codes," in *Proc. IEEE Inform. Theory Workshop (ITW)*, Paris, France, March 2003, pp. 245–248.
- [17] D.A. Spielman, "Linear-time encodable and decodable error-correcting codes," *IEEE Trans. Inf. Theory*, vol. 42, no. 6, pp. 1723–1731, Nov. 1996.
- [18] D. Sridhara and T.E. Fuja, "LDPC codes over rings for PSK modulation," *IEEE Trans. Inf. Theory*, vol. 51, no. 9, pp. 3209–3220, Sep. 2005.
- [19] R.M. Tanner, "A recursive approach to low-complexity codes," *IEEE Trans. Inf. Theory*, vol. 27, no. 5, pp. 533–547, Sep. 1981.
- [20] N. Wiberg, *Codes and Decoding on General Graphs*, Ph.D. Thesis, Linköping University, Sweden, 1996.
- [21] G. Zémor, "On expander codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 835–837, Feb. 2001.

**Vitaly Skachek** was born in Kharkov, Ukraine (former USSR), in 1973. He received the B.A. (Cum Laude), M.Sc. and Ph.D. degrees in computer science from the Technion—Israel Institute of Technology, in 1994, 1998 and 2007, respectively.

During 1996–2002, he held various engineering positions. In the period 2002–2006, he has been working toward the Ph.D. degree at the Computer Science Department at the Technion. In the summer of 2004, he visited the Mathematics of Communications Department at Bell Laboratories under the DIMACS Special Focus Program in Computational Information Theory and Coding. During 2007–2009, Dr. Skachek was a postdoctoral fellow with the Claude Shannon Institute and the School of Mathematical Sciences, University College Dublin. He is now a research fellow with the School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore.

Dr. Skachek is a recipient of the Permanent Excellent Faculty Instructor award, given by Technion.