This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE Globecom 2011 proceedings.

LCD Codes and Iterative Decoding by Projections, a First Step Towards an Intuitive Description of Iterative Decoding

Jalal Etesami, Fangning Hu, and Werner Henkel

Jacobs University Bremen
Electrical Engineering and Computer Science
Transmission Systems Group
Bremen, Germany
Emails: w.henkel@jacobs-university.de
etesami2@uiuc.edu
fangning.hu@hdu.edu.cn
URL: http://trsys.faculty.jacobs-university.de

***Abstract*—From our earlier works, we know that in the case of analog codes, a Turbo-like iterative decoding can be nicely illustrated as iterative projections onto super codes that correspond to parts of the parity check matrix. So-called LCD (linear code with complementary dual) codes are recognized as a counterpart in finite fields for the orthogonal case, where two iterative projections lead to the final solution. A method for decomposing an arbitrary LCD code $\mathcal{C}$ into two super LCD codes $\mathcal{C}_1$ and $\mathcal{C}_2$ such that decoding by iteratively projecting the received vector onto $\mathcal{C}_1$ and $\mathcal{C}_2$ results in the same decoding solution as directly projecting the vector onto the original code space $\mathcal{C}$. This is not necessarily a maximum-likelihood solution opposite to the analog case. A bound on the probability of finding the nearest codeword is provided.**

***Index Terms*—Turbo codes, LDPC codes, Analog codes, iterative decoding, dual code, LCD code**

I. Introduction and Motivation

It is known that in a Galois field, projection is not as well defined as in the real field. A linear code $\mathcal{C}$ over a Galois field can have a dual code $\mathcal{C}^\perp$ such that the intersection of $\mathcal{C}$ and $\mathcal{C}^\perp$ is bigger than $\{\mathbf{0}\}$. A linear code $\mathcal{C}$ with dual code $\mathcal{C}^\perp$ such that $\mathcal{C} \cap \mathcal{C}^\perp = \{\mathbf{0}\}$ was first introduced in [1] which is called a linear code with complementary dual code (or an LCD code). It is shown that the projection onto an LCD can be well defined very similar to the case in the real field.

For the reals, [2]–[4] come to the conclusion that when applying the Turbo-like iterative decoding to an arbitrary analog code by decomposing the original code into an intersection of super spaces is equivalent to projecting the received vector onto these two super spaces and finally results in an optimum least-squares solution. This motivates us to decompose the LCD code into two super LCD codes and decode it by iterative projection. A sufficient condition as well as a method for the decomposition are given for arbitrary LCD codes over arbitrary Galois fields. Furthermore, we proved that the iterative projection results in the same solution as that of directly projecting the received vector to the original LCD code.

The motivation of this work is by no means to propose a new efficient code or decoding algorithm. It is thought as a first step to move an intuitive description that is possible for iterative decoding over real or complex numbers over to finite fields. This intuitive description shows that a Turbo-like decoding of real parallel concatenated codes can be seen as iterative projections, leading to the overall least-squares optimum. Especially, for orthogonal constituent codes the iterations will be a quick two-step process. This paper shows that LCD codes deliver an example over a finite field with an equivalent two-step process. Thus, this example may serve as a first counterpart over finite fields, where the iterative process can be illustrated as projections.

The paper is organized as follows: a basic description of an LCD code is introduced in Section II. In Section III, the sufficient condition for the decomposition is given. The iterative projection decoding will be explained in Section IV and concluding remarks follow in Section V.

II. LCD Codes

A Linear Complementary Dual code (LCD code) is defined to be a linear code $\mathcal{C}$ which has the following property,

$$\mathcal{C} \cap \mathcal{C}^\perp = \{\mathbf{0}\} \,, \tag{1}$$

where $\mathcal{C}^\perp$ is the dual code of the linear code $\mathcal{C}$ [1]. The dual code $\mathcal{C}^\perp$ of a linear space $\mathcal{C}$ is defined as all vectors which are orthogonal to all vectors of $\mathcal{C}$. The dual $\mathcal{C}^\perp$ is the $(n, n-k)$ $\mathbb{F}$-ary linear code if $\mathcal{C}$ is a (n, k) $\mathbb{F}$-ary linear code. In this paper, we always assume a characteristic 2 for $\mathbb{F}$.

$$\mathcal{C}^\perp = \{\mathbf{u} | \mathbf{u}^T \cdot \mathbf{v} = 0, \ \forall \mathbf{v} \in \mathcal{C}\} \,.$$

Now, by the definition of LCD codes in (1), one can conclude,

$$\mathbb{F}^n = \mathcal{C} \oplus \mathcal{C}^\perp \,. \tag{2}$$

978-1-4244-9268-8/11/$26.00 ©2011 IEEE

This means $\mathcal{C}$ is an LCD code when $\mathbb{F}^n$ is the direct sum of $\mathcal{C}$ and $\mathcal{C}^\perp$, i.e., every vector in $\mathbb{F}^n$ can be written uniquely as the sum of a vector in the code space $\mathcal{C}$ and a vector in the dual space $\mathcal{C}^\perp$. Hence, one can define a map from $\mathbb{F}^n$ to $\mathcal{C}$ as

$$T_c : \mathbb{F}^n \mapsto \mathcal{C} \ ,$$

$$T_c\mathbf{v} = \mathbf{c} \Leftrightarrow \mathbf{v} = \mathbf{c} + \acute{\mathbf{c}} \ , \ \mathbf{c} \in \mathcal{C}, \ \acute{\mathbf{c}} \in \mathcal{C}^\perp \ . \tag{3}$$

It is clear that above transformation is well defined by (2) and linear. Hence, there exists such a transformation if and only if $\mathbb{F}^n$ can be written as the direct sum of $\mathcal{C}$ and $\mathcal{C}^\perp$ or equivalently, $\mathcal{C}$ is an LCD code. Due to the linearity of T_c, there exists a matrix representation $\mathbf{P}_c$ for this transformation; matrix $\mathbf{P}_c$ is called the *projection matrix* to $\mathcal{C}$.

$$\mathbf{v}^T\mathbf{P}_c = \mathbf{v}^T \Leftrightarrow \mathbf{v} \in \mathcal{C} \ , \tag{4}$$

$$\mathbf{v}^T\mathbf{P}_c = \mathbf{0}^T \Leftrightarrow \mathbf{v} \in \mathcal{C}^\perp \ .$$

Therefore, if (2) holds, then

$$\exists \ \mathbf{P}_c \in \mathbb{F}^{n\times n}; \forall \mathbf{v} \in \mathbb{F}^n \quad \mathbf{v}^T = \mathbf{v}^T\mathbf{P}_c + (\mathbf{v}^T - \mathbf{v}^T\mathbf{P}_c) \ ,$$

where $\mathbf{v}^T\mathbf{P}_c$ is in $\mathcal{C}$ and $(\mathbf{v}^T - \mathbf{v}^T\mathbf{P}_c)$ is inside $\mathcal{C}^\perp$. Similarly, one can define the projection matrix for $\mathcal{C}^\perp$.

Proposition 1: *If $\boldsymbol{G}$ is a generator matrix of the (n, k) linear code space $\mathcal{C}$, then $\mathcal{C}$ is an LCD code, iff $(\boldsymbol{GG}^T)^{-1}$ exists in $\mathbb{F}^{k\times k}$. Moreover, if $\mathcal{C}$ is an LCD code, then $\boldsymbol{P}_c = \boldsymbol{G}^T(\boldsymbol{GG}^T)^{-1}\boldsymbol{G}$.*

Proof: [1]. □

Proposition 2: *If $\boldsymbol{p} \in \mathbb{F}^{k\times r}$, then $\boldsymbol{G}$ can be defined as the generator matrix of an (n, k) $\mathbb{F}$-ary LCD code.*

$$\mathbf{G} = [\mathbf{I} : \mathbf{p} : \mathbf{p}]_{k\times n} \ , \tag{5}$$

with $(n = k + 2r)$.

Proof: [1]. □

A *parity check matrix* of the generator matrix $\mathbf{G}$ given in (5) is, e.g.,

$$\mathbf{H} = \begin{bmatrix} \mathbf{p}^T & \mathbf{I} & \mathbf{0} \\ \mathbf{p}^T & \mathbf{0} & \mathbf{I} \end{bmatrix}_{(n-k)\times n} . \tag{6}$$

III. Decomposition of LCD Codes

Now, we can expand the code space $\mathcal{C}$ to two super spaces $\mathcal{C}_1$ and $\mathcal{C}_2$ by adding some independent rows to the matrix $\mathbf{G}$, as follows:

$$\mathbf{G}_1 = \begin{bmatrix} \mathbf{G} \\ \mathbf{H}_1 \end{bmatrix} : \mathbb{F}^{k+r} \longmapsto \mathcal{C}_1 \ , \tag{7}$$

$$\mathbf{G}_2 = \begin{bmatrix} \mathbf{G} \\ \mathbf{H}_2 \end{bmatrix} : \mathbb{F}^{k+r} \longmapsto \mathcal{C}_2 \ , \tag{8}$$

where

$$\mathbf{H}_1 = \begin{bmatrix} \mathbf{p}^T & \mathbf{I} & \mathbf{0} \end{bmatrix} \ ,$$

$$\mathbf{H}_2 = \begin{bmatrix} \mathbf{p}^T & \mathbf{0} & \mathbf{I} \end{bmatrix} \ .$$

These expanded code spaces of $\mathcal{C}$ are useful, if

$$\mathcal{C} = \mathcal{C}_1 \cap \mathcal{C}_2 \ . \tag{9}$$

In the following, we will show that by expanding like (7) and (8), (9) will hold. It is easy to check that, if $\mathbf{v}$ is in $\mathcal{C}$, then $\mathbf{v} \in \mathcal{C}_1 \cap \mathcal{C}_2$ because

$$\mathbf{v} = \mathbf{i}^T\mathbf{G} = [\mathbf{i}^T\mathbf{0}^T]\mathbf{G}_1 = [\mathbf{i}^T\mathbf{0}^T]\mathbf{G}_2 \ .$$

For the opposite direction, one can say, if $\mathbf{v} \in \mathcal{C}_1 \cap \mathcal{C}_2$, then there exist $\begin{bmatrix}\mathbf{u}_1^T\mathbf{w}_1^T\end{bmatrix}$ and $\begin{bmatrix}\mathbf{u}_2^T\mathbf{w}_2^T\end{bmatrix}$ in $\mathbb{F}^{k+r}$ such as

$$\mathbf{v}^T = \begin{bmatrix}\mathbf{u}_1^T\mathbf{w}_1^T\end{bmatrix}\mathbf{G}_1 = \begin{bmatrix}\mathbf{u}_2^T\mathbf{w}_2^T\end{bmatrix}\mathbf{G}_2 \ . \tag{10}$$

Therefore, by substituting (7) and (8) into (10), we obtain

$$\mathbf{s}^T = \left(\mathbf{u}_1^T + \mathbf{u}_2^T\right)\mathbf{G} = \begin{bmatrix}\mathbf{w}_1^T\mathbf{w}_2^T\end{bmatrix}\mathbf{H} \ .$$

Above equation says that $\mathbf{s} \in \mathcal{C} \cap \mathcal{C}^\perp = \{\mathbf{0}\}$, therefore $\begin{bmatrix}\mathbf{w}_1^T\mathbf{w}_2^T\end{bmatrix}\mathbf{H} = \mathbf{0}$ and this implies

$$\mathbf{w}_1^T\mathbf{H}_1 = \mathbf{w}_2^T\mathbf{H}_2 \Rightarrow \mathbf{w}_1 = \mathbf{w}_2 = \mathbf{0} \ .$$

The last equality results from the structure of $\mathbf{H}_1$ and $\mathbf{H}_2$. Hence,

$$\mathcal{C} = \mathcal{C}_1 \cap \mathcal{C}_2 \ .$$

Proposition 3: *If $\boldsymbol{p}^T = [\boldsymbol{q} : \boldsymbol{q}]$, $\boldsymbol{q} \in \mathbb{F}^{r\times s}$ and $2s = k$, then $\mathcal{C}_1$ and $\mathcal{C}_2$ are LCD codes.*

Proof: It is enough to show this just for $\mathcal{C}_1$, because $\mathcal{C}_2$ is structurally the same. We have

$$\mathbf{G}_1\mathbf{G}_1^T = \begin{bmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} + \mathbf{p}^T\mathbf{p} \end{bmatrix} \ ,$$

Since $\mathbf{p}^T = [\mathbf{q} : \mathbf{q}]$, we obtain $\mathbf{p}^T\mathbf{p} = \mathbf{0}$. Recall that all operations are in $GF(2)$, therefore $\mathbf{G}_1\mathbf{G}_1^T = \mathbf{I}$ and this is invertible, hence, by Proposition 1, the claim is proven. □

Note: Generally, if one splits an $\mathbf{H}$ matrix into two arbitrary submatrices $\mathbf{H}_1$ and $\mathbf{H}_2$ and define $\mathbf{G}_1$ and $\mathbf{G}_2$ as given below and the condition of Proposition 3 is satisfied, then $\mathcal{C}_1$ and $\mathcal{C}_2$ are LCD codes.

$$\mathbf{G}_1 = \begin{bmatrix} \mathbf{I} & \mathbf{p} & \mathbf{p} \\ \mathbf{A}^T & \mathbf{M} & \mathbf{N} \end{bmatrix}_{(k+r_1)\times n} \ , \tag{11}$$

$$\mathbf{G}_2 = \begin{bmatrix} \mathbf{I} & \mathbf{p} & \mathbf{p} \\ \mathbf{B}^T & \acute{\mathbf{M}} & \acute{\mathbf{N}} \end{bmatrix}_{(k+r_2)\times n} \ , \tag{12}$$

where $r_1 + r_2 = 2r$ and since $\mathbf{H}_1$ and $\mathbf{H}_2$ are submatrices of $\mathbf{H}$, then there exists a permutation matrix $\mathbf{J}$ such that

$$\begin{bmatrix} \mathbf{H}_1 \\ \mathbf{H}_2 \end{bmatrix} = \begin{bmatrix} \mathbf{A}^T & \mathbf{M} & \mathbf{N} \\ \mathbf{B}^T & \acute{\mathbf{M}} & \acute{\mathbf{N}} \end{bmatrix} = \mathbf{J}\begin{bmatrix} \mathbf{p}^T & \mathbf{I} & \mathbf{0} \\ \mathbf{p}^T & \mathbf{0} & \mathbf{I} \end{bmatrix} \ ,$$

If $\mathbf{p}^T = [\mathbf{q} : \mathbf{q}]$, then one obtains the following equations

$$\begin{bmatrix} \mathbf{H}_1 \\ \mathbf{H}_2 \end{bmatrix}\begin{bmatrix} \mathbf{H}_1 \\ \mathbf{H}_2 \end{bmatrix}^T = \mathbf{J}\begin{bmatrix} \mathbf{p}^T & \mathbf{I} & \mathbf{0} \\ \mathbf{p}^T & \mathbf{0} & \mathbf{I} \end{bmatrix}\begin{bmatrix} \mathbf{p} & \mathbf{p} \\ \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} \end{bmatrix}\mathbf{J}^T = \mathbf{I} \ , \tag{13}$$

or equivalently

$$\mathbf{H}_i\mathbf{H}_j^T = \mathbf{0}, i \neq j \ , \tag{14}$$

$$\mathbf{A}^T\mathbf{A} + \mathbf{M}\mathbf{M}^T + \mathbf{N}\mathbf{N}^T = \mathbf{I}_{r_1\times r_1} \ , \tag{15}$$

$$\mathbf{B}^T\mathbf{B} + \acute{\mathbf{M}}\acute{\mathbf{M}}^T + \acute{\mathbf{N}}\acute{\mathbf{N}}^T = \mathbf{I}_{r_2\times r_2} \ . \tag{16}$$

Since $\mathbf{H}_i\mathbf{G}^T = \mathbf{0}, i \in \{1,2\}$, then

$$\mathbf{A}^T + \mathbf{M}\mathbf{p}^T + \mathbf{N}\mathbf{p}^T = \mathbf{0}_{r_1\times k} \tag{17}$$

$$\mathbf{B}^T + \acute{\mathbf{M}}\mathbf{p}^T + \acute{\mathbf{N}}\mathbf{p}^T = \mathbf{0}_{r_2\times k} \ .$$

From equations (14) to (17) and Proposition 1, one can conclude that $\mathbf{G}_1$ and $\mathbf{G}_2$ are LCD codes, moreover, $\mathcal{C} = \mathcal{C}_1 \cap \mathcal{C}_2$, where $\mathcal{C}_i$ is the code space generated by $\mathbf{G}_i$.

$$\mathbf{G}_1\mathbf{G}_1^T = \begin{bmatrix} \mathbf{I} & \mathbf{p} & \mathbf{p} \\ \mathbf{A}^T & \mathbf{M} & \mathbf{N} \end{bmatrix} \begin{bmatrix} \mathbf{I} & \mathbf{A} \\ \mathbf{p}^T & \mathbf{M}^T \\ \mathbf{p}^T & \mathbf{N}^T \end{bmatrix} =$$

$$= \begin{bmatrix} \mathbf{I}_{k\times k} & \mathbf{0}_{k\times r_1} \\ \mathbf{0}_{r_1\times k} & \mathbf{I}_{r_1\times r_1} \end{bmatrix} \ .$$

Note: One can generalize the propositions 2 and 3 to fields with prime characteristic p as the following

$$\mathbf{G} = [\mathbf{I} : \alpha_1\mathbf{p} : \alpha_2\mathbf{p} : \alpha_3\mathbf{p} : \alpha_4\mathbf{p}]_{k\times n} \ ,$$

where $p = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2$ and such numbers exist for any number p by the *Lagrange Theorem*. A corresponding parity-check matrix $\mathbf{H}$ can be

$$\mathbf{H} = \begin{bmatrix} -\alpha_1\mathbf{p}^T & \mathbf{I} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ -\alpha_2\mathbf{p}^T & \mathbf{0} & \mathbf{I} & \mathbf{0} & \mathbf{0} \\ -\alpha_3\mathbf{p}^T & \mathbf{0} & \mathbf{0} & \mathbf{I} & \mathbf{0} \\ -\alpha_4\mathbf{p}^T & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{I} \end{bmatrix} \ .$$

Moreover, if one expands the code space $\mathcal{C}$ to two super spaces like in (7) and (8), then $\mathcal{C}_1$ and $\mathcal{C}_2$ are LCD if

$$\mathbf{p}^T = [\alpha_1\mathbf{q} : \alpha_2\mathbf{q} : \alpha_3\mathbf{q} : \alpha_4\mathbf{q}] \ .$$

IV. Projection and Decoding

Let $\mathbf{v}$ be a code vector from an LCD code space $\mathcal{C}$, transmitted over a noisy channel. At the receiver side, we will have $\mathbf{r} = \mathbf{v} + \mathbf{n}$, where $\mathbf{n}$ is a noise vector with given distribution, then one can obtain a nearest vector in $\mathbb{F}^n$ to $\mathbf{r}$ as the following

$$\mathbf{x} = \arg\min_{\mathbf{y}}\{||\mathbf{y} - \mathbf{r}||_2^2 = \sum_{i=1}^{n}(y_i - r_i)^2\} \ , \tag{18}$$

$$\exists\ \mathbf{e} \in \mathbb{F}^n; \quad \mathbf{x} = \mathbf{v} + \mathbf{e} \quad \textit{modulo } 2 \ . \tag{19}$$

Suppose that $w(\mathbf{e}) \leqslant t$, i.e., the Hamming weight of the error vector $\mathbf{e}$ is smaller than the error correcting capability of the code $\mathcal{C}$, then

$$\arg\min_{\mathbf{y}\in\mathcal{C}}\{||\mathbf{y} - \mathbf{r}||_2^2\} = \arg\min_{\mathbf{y}\in\mathcal{C}}\{||\mathbf{y} - \mathbf{x}||_2^2\} = \mathbf{v} \ . \tag{20}$$

Hence, by Eq. (20), finding the nearest codeword to $\mathbf{r}$ is equal to finding the nearest codeword to the vector $\mathbf{x}$. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two code spaces generated by $\mathbf{G}_1$ and $\mathbf{G}_2$ such that they satisfy (11) and (12) and Proposition 3's condition. Therefore, $\mathcal{C}, \mathcal{C}_1$, and $\mathcal{C}_2$ are LCD codes and there exist projection matrices $\mathbf{P}_c$ and $\mathbf{P}_{ci}$ for the code spaces $\mathcal{C}$ and $\mathcal{C}_i$, hence,

$$\exists\ \ \mathbf{u} \in \mathcal{C};\ \mathbf{x}^T\mathbf{P}_c = \mathbf{u} \quad \textit{modulo } 2 \ ,$$

$$\exists\ \ \mathbf{u}_i \in \mathcal{C}_i;\ \mathbf{x}^T\mathbf{P}_{ci} = \mathbf{u}_i \quad \textit{modulo } 2 \ ,$$

where $\mathbf{P}_{ci} = \mathbf{G}_i^T(\mathbf{G}_i\mathbf{G}_i^T)^{-1}\mathbf{G}_i = \mathbf{G}_i^T\mathbf{G}_i$. However, it is not necessary for $\mathbf{u}$ or $\mathbf{u}_i$ to be equal to $\mathbf{v}$, which is the nearest code vector to $\mathbf{x}$.

A. Iterative Projection between $\mathcal{C}_1$ and $\mathcal{C}_2$.

It has been shown in [3], [4] that the Turbo-like iterative decoding for linear codes defined over the real field can be regarded as iteratively projecting the current estimated vector $\hat{\boldsymbol{x}}(t)$ at iteration t onto two constituent super codes $\mathcal{C}_1$ and $\mathcal{C}_2$ with the original code $\mathcal{C} = \mathcal{C}_1 \cap \mathcal{C}_2$ being the intersection of these two constituent codes. If a linear code is defined in the real field, it can be represented by a hyperplane in the Euclidean space and may be geometrically visualized as a line in Fig. 1. $\mathcal{C}_1$ and $\mathcal{C}_2$ are shown as red and blue lines, respectively, with the intersecting point as the original code $\mathcal{C}$. It can be seen from Fig. 1 that the estimated codeword is first initialized as the received vector $\hat{\boldsymbol{x}}(0) = \boldsymbol{r}$ and the projection process finally converges to the original code space and reaches the least-squares solution $\boldsymbol{x}_{LS}$ when t goes to infinity. Furthermore, if the two constituent code spaces are orthogonal to each other, it only needs two ($t = 2$) iterations to converge.

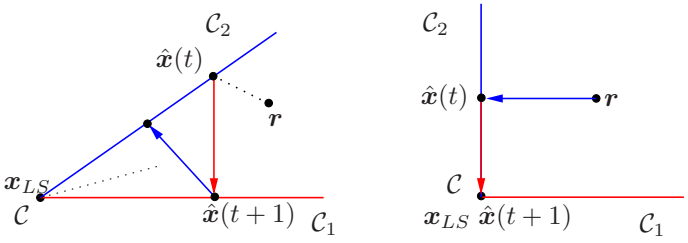

Fig. 1. The geometric illustration of the iterative decoding process in non-orthogonal (left) and orthogonal (right) constituent code spaces.

However, the projection process is not so obvious and intuitive in Galois fields, since unlike the real field where the codewords form a hyperplane which can be easily viewed as a line in the Euclidean space, instead the codewords are lattice points in Galois fields which do not have such a convenient visualization. However, we will show in the following that by decomposing an LCD code into two super LCD codes with their intersection being the original code, iteratively projecting the estimated vector onto these two super code spaces results in the same solution as projecting the estimated vector onto the original code space and it only needs two iterations to converge.

Proposition 4: *If P_{c1}, P_{c2}, and P_c are the projection matrices to the spaces $\mathcal{C}_1$, $\mathcal{C}_2$, and $\mathcal{C}$, generated by $\boldsymbol{G}_1, \boldsymbol{G}_2$, and $\boldsymbol{G}$, respectively, given in (11) and (12), then*

$$\mathbf{x}^T\mathbf{P}_{cj}\mathbf{P}_{ci} = \mathbf{x}^T\mathbf{P},\ j \neq i \in \{1,2\}\ . \tag{21}$$

Proof: $\mathcal{C}$ is an LCD code, therefore, for any $\mathbf{x} \in \mathbb{F}^n$, there exists a vector $\mathbf{v} \in \mathcal{C}$ and a vector $\mathbf{h} \in \mathcal{C}^\perp$, such that

$$\mathbf{x} = \mathbf{v} + \mathbf{h},\ \mathbf{x}^T\mathbf{P}_c = \mathbf{v}^T\ .$$

Since $\mathcal{C} = \mathcal{C}_1 \cap \mathcal{C}_2$, we have $\mathbf{v}^T\mathbf{P}_{ci} = \mathbf{v}^T$, and since $\mathcal{C}_i$ is an LCD code, there exists a vector $[\mathbf{u}_i^T\ \mathbf{h}_i^T] \in \mathbb{F}^{k+r_i}$, such that

$$\mathbf{x}^T\mathbf{P}_{ci} = \mathbf{v}^T + \mathbf{h}^T\mathbf{P}_{ci} = \mathbf{v}^T + [\mathbf{u}_i^T\ \mathbf{h}_i^T]\begin{bmatrix}\mathbf{G}\\ \mathbf{H}_i\end{bmatrix}\ , \tag{22}$$

since $\mathcal{C}_i^\perp \subseteq \mathcal{C}^\perp$, then $[\mathbf{u}_i^T\ \mathbf{h}_i^T]\begin{bmatrix}\mathbf{G}\\ \mathbf{H}_i\end{bmatrix} \in \mathcal{C}_i \cap \mathcal{C}^\perp$, $\mathbf{u}_i$ must be a zero vector. Now, if one projects (22) again onto the space $\mathcal{C}_j$ by applying $\mathbf{P}_{cj}$ where $i \neq j$, then the result is the following

$$\mathbf{x}^T\mathbf{P}_{ci}\mathbf{P}_{cj} = \mathbf{v}^T + [\mathbf{0}^T\ \mathbf{h}_i^T]\mathbf{G}_i\mathbf{P}_{cj}\ , \tag{23}$$

$$\mathbf{P}_{cj} = \mathbf{G}_j^T(\mathbf{G}_j\mathbf{G}_j^T)^{-1}\mathbf{G}_j\ ,$$

However, from (14), one can obtain

$$\mathbf{G}_i\mathbf{G}_j^T = \begin{bmatrix}\mathbf{G}\\ \mathbf{H}_i\end{bmatrix}\begin{bmatrix}\mathbf{G}^T & \mathbf{H}_j^T\end{bmatrix} = \begin{bmatrix}\mathbf{I} & \mathbf{0}\\ \mathbf{0} & \mathbf{0}\end{bmatrix}\ .$$

Hence, the second term on the right hand side of (23) would be zero. □

This means that iteratively projecting the vector $\mathbf{x}$ onto $\mathcal{C}_1$ and $\mathcal{C}_2$ after two iterations is equivalent to projecting $\mathbf{x}$ directly onto $\mathcal{C}$.

B. Projection directly onto $\mathcal{C}$.

$\mathbb{F}^n$ is a direct sum of $\mathcal{C}$ and $\mathcal{C}^\perp$, therefore, $\mathbf{e}$ can be written as the sum of a vector in $\mathcal{C}$ and a vector in $\mathcal{C}^\perp$. Hence, there exist $\mathbf{z} \in \mathbb{F}^k$ and $\mathbf{t} \in \mathbb{F}^{n-k}$, such that $\mathbf{e}^T = \mathbf{z}^T\mathbf{G} + \mathbf{t}^T\mathbf{H}$, therefore,

$$\mathbf{x}^T\mathbf{P}_c = (\mathbf{v}^T + \mathbf{e}^T)\mathbf{P}_c = \tag{24}$$

$$= \mathbf{v}^T + \mathbf{z}^T\mathbf{G}\ .$$

By Eq. (24), one can conclude that $\mathbf{x}^T\mathbf{P}_c$ is the nearest codeword to the received vector $\mathbf{x}$ iff $\mathbf{z} = \mathbf{0}$, i.e., $\mathbf{e} \in \mathcal{C}^\perp$. This will happen with a certain probability which is bounded as follows:

$$P\left(\mathbf{x}^T\mathbf{P}_c = \arg\min_{\mathbf{y}\in\mathcal{C}}\{||\mathbf{y}-\mathbf{r}||_2^2\}\right) =$$

$$= P(\mathbf{e} \in \mathcal{C}^\perp | \mathbf{e} = \mathbf{x} + \mathbf{v}) \leqslant P(\mathbf{e} \in \mathcal{C}^\perp) = \frac{2^{n-k}}{2^n} = \frac{1}{2^k}\ .$$

V. Conclusions

LCD codes provided a counterpart for iterative decoding similar to the analog coding case [3], [4], where a split of a parity-check matrix leads to super codes and iterative decoding between them was shown to lead to a least-squares optimum in the form of iterative projections (not always orthogonal) onto the super codes. In case of orthogonal super codes, two orthogonal projections lead to the final result. The presented LCD code construction exactly offers a similar result. Also there, two projections lead to the final result, however, not necessarily an optimum one. Nevertheless, a single projection would also lead to the same result as the two iterative ones onto super codes.

Our intention was to find a counterpart to the iterative projections representing a Turbo-like procedure over a finite field that we had previously found with analog codes over complex numbers. We have pointed out that an LCD code construction has the corresponding properties. This result may serve as just one step-stone towards a more intuitive understanding of iterative decoding, that is already present for the complex case. The projection decoding was not investigated to obtain an improved decoding algorithm. Neither the code construction nor the decoding algorithm are thought for practical applications, only as a tool for a more intuitive understanding.

Acknowledgment

This work is funded by the German National Science Foundation (Deutsche Forschungsgemeinschaft, DFG).

We thank Prof. Jim Massey for pointing us to his early works on linear codes with complementary duals.

References

[1] J. Massey, "Linear Codes with Complementary Duals," *Discrete Mathematics*, Vol. 106/107, pp. 337-342, 1992.

[2] M. Mura, W. Henkel,, L. Cottatellucci, "Iterative Least-squares Decoding of Analog Product Codes," proc. *IEEE International Symposium on Information Theory, ISIT 2003* pp. 44, June 29 - July 4, 2003.

[3] F. Hu and W. Henkel, "Turbo-like Iterative Least-Squares Decoding to Analog Codes," *IEEE Electronics Letter.*, Vol. 41, No. 22, pp. 1233 - 1234, Oct. 27, 2005.

[4] F. Hu and W. Henkel, "An Analysis of the Sum-Product Decoding of Analog Compound Codes," 2007 IEEE International Symposium on Information Theory (ISIT 2007), Nice, France, pp. 1886 - 1890, June 24-29, 2007.