ISIT'2013 1569716285

Bit-error Resilient Index Assignment for Multiple Description Scalar Quantizers

Sorina Dumitrescu and Yinghan Wan
Electrical and Computer Engineering Department, McMaster University, Canada
Email: sorina@mail.ece.mcmaster.ca; katrina@grads.ece.mcmaster.ca

***Abstract*—This work addresses the problem of increasing the robustness to bit errors for two description scalar quantizers. To this aim a permutation is applied to the indices of each description. We show how to construct permutation pairs that increase the minimum Hamming distance of the set of valid index pairs to 3 when the redundancy is sufficiently high.**

Additionally, for the case when one description is known to be correct we propose a new performance criterion, denoted by $d_{side,min}$. This represents the minimum Hamming distance of the set of valid indices of one description, when the index of the other description is fixed. We develop a technique for constructing permutation pairs achieving $d_{side,min} \geq h$ based on a linear $(R, \lceil \log_2 m \rceil)$ channel code of minimum Hamming distance $h+1$, where R is the rate of each description and m is the number of diagonals occupied by the valid index pairs in the matrix of the initial index assignment.

I. Introduction

In the multiple description (MD) problem the goal is to generate a given number of descriptions of a signal, such that each separate description leads to a reconstruction of acceptable quality, while more descriptions refine each other improving the reconstruction. While MD schemes traditionally target robustness against losses, a natural question is whether the redundancy that is intentionally built into the system can also be used to combat other channel impairments, such as bit-errors.

Indeed, the ability of combatting bit errors (with or without additional channel coding) has been attested to and exploited via joint source-channel decoding [1], [2]. On the other hand, the design of MD codes to strengthen this ability has received attention only very recently [3], [4]. The authors of [3] consider the case of a two description scalar quantizer (2DSQ) and identify as a measure for index assignment (IA) robustness to bit errors, the minimum Hamming distance of the set of valid pairs of two description indices. They propose a genetic algorithm to heuristically assign central partition cells to index pairs. As for the problem of finding sets of index pairs of minimum Hamming distance equal to some given value h, they propose a solution only when $h = 2$. In [4] the authors consider a multiple description scalar quantizer with a general number of descriptions and optimize the IA taking into account the source and channel statistics using the binary switching heuristic algorithm.

This work addresses the problem of increasing the bit-error resilience of the IA in the case of balanced 2DSQ, without decreasing its resilience to description loss. Our approach is to start from an initial IA which is known to be good for the conventional 2DSQ problem, such as the IA's proposed in [5], [8], and apply a permutation to the indices of each description. Such a technique does not change the performance of the 2DSQ in the conventional sense, i.e., when the descriptions are not corrupted by bit errors, but it has the potential of increasing the bit error resilience at the central decoder.

For the scenario when both descriptions may carry bit errors we use the minimum Hamming distance of the set of valid index pairs, denoted by d_{min}, as a performance measure, following [3]. We will show how to construct permutation pairs which achieve $d_{min} = 3$, for initial IA's with high enough redundancy. Using such permutations the central decoder is able to correct any one bit error pattern in the pair of received indexes.

Another interesting scenario is when one description is known to be correct. For this scenario we propose a better suited performance criterion, termed the *side minimum Hamming distance* of the IA, and denoted by $d_{side,min}$. This notion is defined as the minimum Hamming distance of the set of valid indices of the description which may carry errors, when the index in the correct description is fixed. We show how to construct a permutation pair achieving $d_{side,min} \geq h$ based on a linear $(R, \lceil \log_2 m \rceil)$ channel code of minimum Hamming distance $h+1$, where R is the rate of each description and m is the number of diagonals occupied by the valid index pairs in the initial IA matrix. We additionally prove that for any linear permutation the achievable $d_{side,min}$ cannot be higher than the largest minimum Hamming distance of a linear $(R, \lceil \log_2 m \rceil)$ channel code.

II. Definitions and Notations

Let $\mathbb{F}_2$ denote the binary field with elements 0 and 1. We use lower case letters in bold to denote bit sequences. If the length of the bit sequence $\mathbf{u}$ is k then we write $\mathbf{u} = (u_1, u_2, \cdots u_k)$. Note that $\mathbf{u}$ is a row vector in the vector space $\mathbb{F}_2^k$. Additionally, denote $\mathbf{u}_s^t = (u_s, u_{s+1}, \cdots u_t)$, for any $1 \leq s \leq t \leq k$. For every integers i and $k > 0$ such that $0 \leq i \leq 2^k - 1$, $\boldsymbol{\beta}_k(i)$ denotes the k bit representation of i starting with the most significant bit and ending with the least significant bit. When $k = R$ we will omit the subscript, i.e., we will use $\boldsymbol{\beta}(i)$ instead of $\boldsymbol{\beta}_R(i)$. Conversely, for any bit sequence $\mathbf{b} \in \mathbb{F}_2^k$, $k > 0$, $i(\mathbf{b})$ denotes the corresponding integer in natural binary representation, i. e., $i(\mathbf{b}) \triangleq \sum_{s=1}^{k} b_s 2^{k-s}$. For any positive integer k, $\mathbf{0}_k$, respectively $\mathbf{1}_k$, denotes the all zero, respectively

all one, vector in $\mathbb{F}_2^k$. The subscript k will be omitted when it is understood from the context.

We will use upper case letters in bold to denote matrices with elements in $\mathbb{F}_2$. The set of all n-by-k matrices with elements in $\mathbb{F}_2$ is denoted by $\mathcal{M}_{n\times k}$. $\mathbf{I}_k$ denotes the k-by-k identity matrix, $\mathbf{0}_{n\times k}$ denotes the n-by-k zero matrix, and $\mathbf{D}_k$ denotes the matrix in $\mathcal{M}_{k\times k}$ with elements $D(i,j)=1$ if and only if $i=j$ or $i=j-1$. For any matrix $\mathbf{A}$, $\mathbf{A}^T$ denotes its transpose.

The addition of integers is denoted by "+", while the addition in the binary field $\mathbb{F}_2$ is denoted by "$\oplus$". The component wise addition of vectors in $\mathbb{F}_2^k$ and of matrices in $\mathcal{M}_{n\times k}$ are also denoted by "$\oplus$". For any two sets $\mathcal{A},\mathcal{B}\subseteq\mathbb{F}_2^k$, we define their sum $\mathcal{A}\oplus\mathcal{B}\triangleq\{u\oplus v: u\in\mathcal{A}, v\in\mathcal{B}\}$ (**note**: this should not be confused with the notion of direct sum).

For any binary vector $\mathbf{u}\in\mathbb{F}_2^k$, $k>0$, its Hamming weight $H(\mathbf{u})$ is defined as the number of components equal to 1. The Hamming distance between two binary vectors $\mathbf{u}$ and $\mathbf{v}$ of the same dimension is $d(\mathbf{u},\mathbf{v})\triangleq H(\mathbf{u}\oplus\mathbf{v})$. For any set $\mathcal{A}\subseteq\mathbb{F}_2^k$, define $H_{min}(\mathcal{A})=\min_{\mathbf{u}\in\mathcal{A}}H(\mathbf{u})$. Additionally, if $|\mathcal{A}|\geq 2$, denote by $d_{min}(\mathcal{A})$ the minimum Hamming distance between any two different elements of $\mathcal{A}$.

The encoder of a balanced two description scalar quantizer (2DSQ) operates as follows. The source sample x is encoded first by a so-called central quantizer q to an index $k\in\{0,\cdots,N-1\}$. Every index k is further mapped to an index pair (i,j) via the index assignment mapping $\alpha:\{0,\cdots,N-1\}\to\{0,\cdots,2^R-1\}\times\{0,\cdots,2^R-1\}$, where R is a positive integer. Further, the R-bit binary representation of i, respectively j, represents description 1, respectively 2, and is sent over channel 1, respectively 2. We will denote by $Im(\alpha)$ the set of assigned index pairs, i.e., $Im(\alpha)=\{\alpha(k): 0\leq k\leq N-1\}$.

In a conventional 2DSQ it is assumed that each channel either transmits correctly or breaks down. Therefore, at the receiver end there are three decoders, one for each non-empty subset of received descriptions: the central decoder g_0 (when both i and j are received) and the side decoders g_1 (when only i is received) and g_2 (when only j is received). The trade off between the quality of the reconstruction at the three decoders is controlled by the number N of central quantizer cells and by the IA α. Good IA's were investigated in [5]–[8].

In the case when the descriptions may also be affected by bit errors the redundancy between descriptions can be used at the central decoder to improve the reconstruction. For this we propose to introduce a minimum Hamming distance decoder before g_0. More precisely, if (i',j') is the index pair arriving at the central decoder, then we first look for the valid pair $(\hat{i},\hat{j})\in Im(\alpha)$ such that $(\boldsymbol{\beta}(\hat{i}),\boldsymbol{\beta}(\hat{j}))$ is closest in Hamming distance to $(\boldsymbol{\beta}(i'),\boldsymbol{\beta}(j'))$. After that the decoding mapping g_0 is applied to $(\hat{i},\hat{j})$. Let us denote $d_{min}(\alpha)\triangleq d_{min}(\{(\boldsymbol{\beta}(i),\boldsymbol{\beta}(j)):(i,j)\in Im(\alpha)\})$. Then it is clear that $d_{min}(\alpha)$ can be used as a measure of robustness to bit errors of the IA α. Specifically, the central decoder can correct all error patterns with at most $\left\lceil\frac{d_{\min}(\alpha)}{2}\right\rceil-1$.

On the other hand, for the situation when one description is known to be correct we propose a better performance measure. Let us assume that description 1 is known to be correct and let (i,j') be the index pair received at the central decoder. Then the minimum Hamming distance decoder needs to look only in the set $\{j:(i,j)\in Im(\alpha)\}$ for the index $\hat{j}$ such that $\boldsymbol{\beta}(\hat{j})$ is closest in Hamming distance to $\boldsymbol{\beta}(j')$. Then a relevant performance measure is what we will refer to as the *side 2 minimum Hamming distance* denoted by $d_{2,\min}(\alpha)$ and defined as

$$d_{2,\min}(\alpha)\triangleq\min_{i\in\{0,1,\cdots,2^R-1\}}d_{\min}(\{\boldsymbol{\beta}(j):(i,j)\in Im(\alpha)\}).$$

Clearly, the minimum Hamming distance decoder is able to correct any error pattern with at most $\left\lceil\frac{d_{2,\min}(\alpha)}{2}\right\rceil-1$ bit errors.

It is clear that for any IA α, we have $d_{2,\min}(\alpha)\geq d_{\min}(\alpha)$ and it can be shown that there are IA's of interest where the inequality is strict. The side 1 minimum Hamming distance $d_{1,\min}(\alpha)$ is defined similarly. Additionally, we define $d_{side,\min}(\alpha)\triangleq\min(d_{1,\min}(\alpha),d_{2,\min}(\alpha))$.

In order to increase the robustness when the channels may additionally introduce bit-errors, while maintaining the performance of the 2DSQ in the bit error-free case we start with an IA known to be good for the conventional 2DSQ and apply an index permutation to the index output by each description. Let $\pi_s:\{0,1,\cdots,2^R-1\}\to\{0,1,\cdots,2^R-1\}$ be the permutation applied to indices of description s, $s=1,2$. We will use the notation $\boldsymbol{\pi}$ for the permutation pair (π_1,π_2). Thus, a new IA, denoted by $\boldsymbol{\pi}\circ\alpha$, is generated, where for any $k\in\{0,1,\cdots,N-1\}$ we have $(\boldsymbol{\pi}\circ\alpha)(k)=(\pi_1(i),\pi_2(j))$, where $(i,j)=\alpha(k)$.

We will consider initial IA's with the assigned pairs filling the main diagonal and the closest $m-1$ diagonals in the IA matrix, as advocated in [5], [8]. We will refer to such IA's as m-diagonal IA's, formally defined as follows.

Definition 1. *For $2\leq m\leq 2^R$, an m-diagonal IA is an IA α, where $Im(\alpha)$ is the set of all pairs $(a,a+\tau)$ satisfying $0\leq a\leq 2^R-1$ and $\max(-a,-m+1+\lfloor\frac{m}{2}\rfloor)\leq\tau\leq\min(\lfloor\frac{m}{2}\rfloor,2^R-1-a)$.*

It can be easily verified that for any m-diagonal IA α with $m\geq 2$, one has $d_{min}(\alpha)=d_{1,min}(\alpha)=d_{2,min}(\alpha)=1$.

Since it is desirable to have simple constructions for the permutations π_s, we will consider in this work permutations which correspond to linear transformations of the vector space $\mathbb{F}_2^R$. The formal definition follows.

Definition 2. *An one-to-one mapping $\pi:\{0,1,\cdots,2^R-1\}\to\{0,1,\cdots,2^R-1\}$ is called linear permutation if there is a full rank matrix $G_\pi\in\mathcal{M}_{R\times R}$ such that $\boldsymbol{\beta}(\pi(j))=\boldsymbol{\beta}(j)G_\pi$, for any $0\leq j\leq 2^R-1$.*

III. Permutations that Increase the Side Minimum Hamming Distance

Definition 3. *For any integers $R\geq 2$, $2\leq m\leq 2^R$, and any one-to-one mapping $\pi:\{0,\cdots,2^R-1\}\to\{0,\cdots,2^R-1\}$,*

define

$$\mu(\pi,m) \triangleq \min_{\substack{j_1,j_2\in\{0,1,\cdots,2^R-1\}\\ 1\le|j_1-j_2|\le m-1}} d(\boldsymbol{\beta}(\pi(j_1)),\boldsymbol{\beta}(\pi(j_2))). \quad (1)$$

It can be easily seen that for any permutation pair $\boldsymbol{\pi} = (\pi_1,\pi_2)$ and any m-diagonal IA α, one has

$$d_{1,\min}(\boldsymbol{\pi}\circ\alpha) = \mu(\pi_1,m), \quad d_{2,\min}(\boldsymbol{\pi}\circ\alpha) = \mu(\pi_2,m).$$

Therefore, we will focus on developing linear permutations π with large $\mu(\pi,m)$.

Definition 4. *For any integers R and k, $1\le k\le R$, and any matrix $\mathbf{A}\in\mathcal{M}_{k\times R}$ with $rank(\mathbf{A})=k$, define*

$$\mathcal{S}(\mathbf{A}) \triangleq \{\mathbf{bA} : \mathbf{b} = (\mathbf{0}_{k-t},\mathbf{1}_t), 1\le t\le k\}.$$

Additionally, for any integer m, $2\le m\le 2^k$, define

$$\mathcal{V}(m,\mathbf{A}) \triangleq \{\mathbf{bA} : \mathbf{b}\in\mathbb{F}_2^k, i(\mathbf{b})\ge 2^k-m+1\}.$$

We will use the notation $d_{min}(\mathbf{A})$ for the minimum Hamming distance of the linear code generated by matrix $\mathbf{A}$. The following result provides a simpler way for determining the value of $\mu(\pi,m)$ for a linear permutation π.

Theorem 1. *Consider integers $R\ge 3$ and $m, 2\le m\le 2^R$. Let $\mathbf{G}\in\mathcal{M}_{R\times R}$ be a full rank matrix. Let $k=\lceil\log_2 m\rceil$ and denote by $\mathbf{A}$, respectively $\mathbf{B}$, the submatrix of $\mathbf{G}$ formed out of the first $R-k$ rows, respectively last k rows. Then the linear permutation π defined by $\mathbf{G}$ has the following property*

$$\mu(\pi,m) = \min\{d_{min}(\mathbf{B}), H_{min}(\mathcal{S}(\mathbf{A})\oplus\mathcal{V}(m,\mathbf{B}))\}. \quad (2)$$

Proof: We will first show that inequality "$\ge$" holds between the expressions in (2). For this we have to show that for any $a\in\{0,\cdots,2^R-2\}$ and $\tau\in\{1,2,\cdots,\min(m-1,2^R-a-1)\}$ the inequality

$$H((\boldsymbol{\beta}(a)\oplus\boldsymbol{\beta}(a+\tau))\mathbf{G}) \ge \min\{d_{min}(\mathbf{B}), H_{min}(\mathcal{S}(\mathbf{A})\oplus\mathcal{V}(m,\mathbf{B}))\}, \quad (3)$$

is valid. Let us fix arbitrary a and τ as above and consider the unique integers c and e such that $a = c\times 2^k+e$, $0\le c\le 2^{R-k}-1$ and $0\le e\le 2^k-1$. Then $\boldsymbol{\beta}(a) = (\boldsymbol{\beta}_{R-k}(c),\boldsymbol{\beta}_k(e))$ and one of the following two cases is possible: $e+1\le e+\tau\le 2^k-1$ or $2^k\le e+\tau\le 2^{k+1}-1$.

Case 1: $e+1\le e+\tau\le 2^k-1$. Then $\boldsymbol{\beta}(a+\tau) = (\boldsymbol{\beta}_{R-k}(c),\boldsymbol{\beta}_k(e+\tau))$, leading to $\boldsymbol{\beta}(a)\oplus\boldsymbol{\beta}(a+\tau) = (\mathbf{0}_{R-k},\boldsymbol{\beta}_k(e)\oplus\boldsymbol{\beta}_k(e+\tau))$, and $\boldsymbol{\beta}_k(e)\oplus\boldsymbol{\beta}_k(e+\tau)\ne\mathbf{0}_k$. This implies that

$$H((\boldsymbol{\beta}(a)\oplus\boldsymbol{\beta}(a+\tau))\mathbf{G}) = H((\boldsymbol{\beta}_k(e)\oplus\boldsymbol{\beta}_k(e+\tau))\mathbf{B}) \ge d_{min}(\mathbf{B}). \quad (4)$$

Case 2: $2^k\le e+\tau\le 2^{k+1}-1$. Then one has $\boldsymbol{\beta}(a+\tau) = (\boldsymbol{\beta}_{R-k}(c+1),\boldsymbol{\beta}_k(e+\tau-2^k))$. Then relation $\boldsymbol{\beta}_{R-k}(c+1) = \boldsymbol{\beta}_{R-k}(c)\oplus(\mathbf{0}_{s-1},\mathbf{1}_{R-k-s+1})$ holds, where s denotes the position of the rightmost 0 in $\boldsymbol{\beta}_{R-k}(c)$ (thus, $1\le s\le R-k$). It follows that

$$(\boldsymbol{\beta}(a)\oplus\boldsymbol{\beta}(a+\tau))\mathbf{G} = (\mathbf{0}_{s-1},\mathbf{1}_{R-k-s+1})\mathbf{A}\oplus\mathbf{bB}, \quad (5)$$

where $\mathbf{b} = \boldsymbol{\beta}_k(e)\oplus\boldsymbol{\beta}_k(e+\tau-2^k)$. Clearly, $(\mathbf{0}_{s-1},\mathbf{1}_{R-k-s+1})\mathbf{A}\in\mathcal{S}(\mathbf{A})$. Additionally, using the fact that $i(\mathbf{b}_1\oplus\mathbf{b}_2)\le i(\mathbf{b}_1)+i(\mathbf{b}_2)$ for any $\mathbf{b}_1,\mathbf{b}_2\in\mathbb{F}_2^k$, it follows that $e = i(\mathbf{b}\oplus\boldsymbol{\beta}_k(e+\tau-2^k))\le i(\mathbf{b})+(e+\tau-2^k)$. This implies that $i(\mathbf{b})\ge 2^k-\tau\ge 2^k-m+1$, and further that $\mathbf{bB}\in\mathcal{V}(m,\mathbf{B})$. Thus, (5) leads to

$$H((\boldsymbol{\beta}(a)\oplus\boldsymbol{\beta}(a+\tau))\mathbf{G}) \ge H_{min}(\mathcal{S}(\mathbf{A})\oplus\mathcal{V}(m,\mathbf{B})). \quad (6)$$

Relations (4) and (6) imply (3).

Next we will show that

$$\mu(\pi,m)\le d_{min}(\mathbf{B}). \quad (7)$$

For this it is sufficient to prove that for any $\mathbf{b} = (b_1,\cdots,b_k)\in\mathbb{F}_2^k\setminus\{\mathbf{0}_k\}$ there are $a\in\{0,\cdots,2^R-2\}$ and $\tau\in\{1,2,\cdots,\min(m-1,2^R-a-1)\}$ such that $\boldsymbol{\beta}(a)\oplus\boldsymbol{\beta}(a+\tau) = (\mathbf{0}_{R-k},\mathbf{b})$. Assume first that $b_1=0$. Then $1\le i(\mathbf{b})\le 2^{k-1}-1\le m-1$. Thus, we may take $\tau = i(\mathbf{b})$. Let $a = c\times 2^k$ for some c such that $0\le c\le 2^{R-k}-1$. Then $a+\tau = c\times 2^k+i(\mathbf{b})$ and it is clear that the requirements on a and τ are satisfied.

Now assume that $b_1=1$. Then $2^k-1\ge i(\mathbf{b})\ge 2^{k-1}$, which implies that $1\le 2^k-i(\mathbf{b})\le 2^{k-1}\le m-1$. Thus, we may take $\tau = 2^k-i(\mathbf{b})$ and $a = c\times 2^k+i(\mathbf{b})-2^{k-1}$ for some c such that $0\le c\le 2^{R-k}-1$. Then $a+\tau = c\times 2^k+2^{k-1}$ and it follows that the desired requirements are satisfied. Thus, the proof of (7) is completed.

To complete the proof of the Theorem it remains to show that

$$\mu(\pi,m)\le H_{min}(\mathcal{S}(\mathbf{A})\oplus\mathcal{V}(m,\mathbf{B})). \quad (8)$$

For this it is sufficient to prove that for any s, $1\le s\le R-k$ and any $\mathbf{b} = (b_1,\cdots,b_k)\in\mathbb{F}_2^k$ satisfying $i(\mathbf{b})\ge 2^k-m+1$, there are integers $a\in\{0,\cdots,2^R-2\}$ and $\tau\in\{1,2,\cdots,\min(m-1,2^R-a-1)\}$ such that $\boldsymbol{\beta}(a)\oplus\boldsymbol{\beta}(a+\tau) = (\mathbf{0}_{s-1},\mathbf{1}_{R-k-s+1},\mathbf{b})$. Let us fix such an s and $\mathbf{b}$. The fact that $i(\mathbf{b})\ge 2^k-m+1$ implies that $2^k-i(\mathbf{b})\le m-1$. Thus, we may choose $\tau = 2^k-i(\mathbf{b})$ and $a = c\times 2^k+i(\mathbf{b})$, where $c = 2^{R-k-s}-1$. Then $a+\tau = (c+1)\times 2^k$ and $\boldsymbol{\beta}(a)\oplus\boldsymbol{\beta}(a+\tau) = (\mathbf{0}_{s-1},\mathbf{1}_{R-k-s+1},\mathbf{b})$. It follows that $(\boldsymbol{\beta}(a)\oplus\boldsymbol{\beta}(a+\tau))\mathbf{G} = (\mathbf{0}_{s-1},\mathbf{1}_{R-k-s+1})\mathbf{A}\oplus\mathbf{bB}$ holds, fact which implies (8). Finally, relations (3), (7) and (8) lead to the conclusion that (2) holds, thus completing the proof. ■

Notation: For any integers $R\ge 2$ and $1\le k\le R$ let $d_{lin}(R,k)$ denote the largest minimum distance of a linear (R,k) channel code. For any integers $R\ge 3$ and $m, 2\le m\le 2^R$ let $\delta_{lin}(R,m)$, denote the maximum value of $\mu(\pi,m)$ over all linear permutations π of the set $\{0,\cdots,2^R-1\}$.

Corollary 1. *Consider integers $R\ge 3$ and $m, 2\le m\le 2^R$. Let $k=\lceil\log_2 m\rceil$. Then the following relations hold*

$$d_{lin}(R,k)-1\le\delta_{lin}(R,m)\le d_{lin}(R,k).$$

Proof: The second inequality follows from Theorem 1. In order to prove the first inequality construct the permutation matrix $\mathbf{G}$ as follows. $\mathbf{G} = [\mathbf{A}^T\ \mathbf{B}^T]^T$, where $\mathbf{A} = [\mathbf{0}_{(R-k)\times k}\ \mathbf{D}_{R-k}]$ and $\mathbf{B}$ is the generator matrix

of an (R,k) channel code of minimum distance $d_{lin}(R,k)$, $\mathbf{B}=[\mathbf{I}_k\ \mathbf{P}_{k\times(R-k)}]$. Then any vector in $\mathcal{S}(\mathbf{A})$ has Hamming weight 1, thus any vector in $\mathcal{S}(\mathbf{A})\oplus\mathcal{V}(m,\mathbf{B})$ has Hamming weight at least $d_{lin}(R,k)-1$. Now the conclusion follows by applying Theorem 1. ∎

The next result exploits the technique developed in the above proof to construct permutations π achieving $\mu(\pi,m)$ larger or equal to 2, respectively 3, based on shortened Hamming codes.

Proposition 1. *Let $R\geq 3$ and $m\geq 2$ be integers.*

1) *If $\lceil\log_2 m\rceil \leq \min(R-2, R-\log_2(R+1))$ then $\delta_{lin}(R,m)\geq 2$.*
2) *If $\lceil\log_2 m\rceil \leq \min(R-3, R-1-\log_2 R)$ then $\delta_{lin}(R,m)\geq 3$.*

Proof: 1) Let $k=\lceil\log_2 m\rceil$, $m'=R-k$ and $l=2^{m'}-1-R$. The condition $\lceil\log_2 m\rceil\leq\min(R-2,R-\log_2(R+1))$ implies that $m'\geq 2$ and $l\geq 0$. Notice that $R=2^{m'}-l-1$, while $k=2^{m'}-l-1-m'$. Thus, there exists a shortened (R,k) Hamming code of minimum distance at least equal to 3 [9]. Corollary 1 leads further to the desired conclusion.

2) Consider m' and l as above. Then the condition $\lceil\log_2 m\rceil\leq\min(R-3,R-1-\log_2 R)$ implies that $m'\geq 3$ and $l\geq 2^{m'-1}-1$. Thus, there exists a shortened (R,k) Hamming code of minimum distance at least equal to 4 [9]. The conclusion now follows via Corollary 1. ∎

IV. Permutations for Achieving a Minimum Hamming Distance of 3

Proposition 2. *Let R and $m\geq 2$ be positive integers such that $2^{\lceil\log_2 m\rceil}(\lceil\log_2 m\rceil+2)\leq 2^{R-5}$. Then there is a pair $\boldsymbol{\pi}=(\pi_1,\pi_2)$ of linear permutations of the set $\{0,\cdots,2^R-1\}$, such that $d_{min}(\boldsymbol{\pi}\circ\alpha)\geq 3$ for any m-diagonal IA α.*

Proof: Let $k=\lceil\log_2 m\rceil$. Construct the matrix $\mathbf{G}_i$ corresponding to permutation π_i as $\mathbf{G}_i=[\mathbf{A}_i^T\mathbf{B}_i^T]^T$, for $i=1,2$, where $\mathbf{A}_i$ and $\mathbf{B}_i$ are described next. $\mathbf{A}_1\in\mathcal{M}_{(R-k)\times R}$ with $\mathbf{A}_1=[\mathbf{0}_{(R-k)\times k}\ \mathbf{D}_{R-k}]$ and $\mathbf{B}_1\in\mathcal{M}_{k\times R}$ with $\mathbf{B}_1=[\mathbf{I}_k\ \mathbf{P}_1]$ where $\mathbf{P}_1$ satisfies the following properties:
C1) Any two rows of $\mathbf{P}_1$ are different and the Hamming weight of any row of $\mathbf{P}_1$ is an odd number larger or equal to 3. **C2)** If the Hamming weight of a row of $\mathbf{P}_1$ is 3 then the last component of that row is 0. **C3)** Every row of $\mathbf{P}_1$ starts with $(1,0,1)$.

Property **C1** implies that $d_{min}(\mathbf{B}_1)\geq 4$ [9]. Notice that the total possible number of vectors in $\mathbb{F}_2^{R-k}$ satisfying properties **C1-C3** is $2^{R-k-4}-1$. Therefore, such a matrix $\mathbf{P}_1$ exists if and only if $R-k\geq 5$ and $k\leq 2^{R-k-4}-1$, conditions which are satisfied by the hypothesis.

Matrix $\mathbf{G}_2$ is constructed such that $\mathbf{A}_2\in\mathcal{M}_{(R-k-1)\times R}$ with $\mathbf{A}_2=[\mathbf{0}_{(R-k-1)\times(k+1)}\ \mathbf{D}_{R-k-1}]$ and $\mathbf{B}_2\in\mathcal{M}_{(k+1)\times R}$ with $\mathbf{B}_2=[\mathbf{I}_{k+1}\ \mathbf{P}_2]$ where $\mathbf{P}_2$ has the following properties: **C4)** Any two rows of $\mathbf{P}_2$ are different and the Hamming weight of any row of $\mathbf{P}_2$ is an odd number larger or equal to 3. **C5)** Every row of $\mathbf{P}_2$ starts with $(0,1,0)$.

Property **C4** implies that $d_{min}(\mathbf{B}_2)\geq 4$ [9]. Notice that the total possible number of vectors in $\mathbb{F}_2^{R-k}$ satisfying properties **C4** and **C5** is $2^{R-k-5}-1$. Therefore, the conditions imposed in the hypothesis imply that such a matrix $\mathbf{P}_2$ exists.

Consider two pairs of valid indices $(a,a+\tau)$ and $(a',a'+\tau')$ satisfying Definition 1. Then we have to prove that

$$H((\boldsymbol{\beta}(a)\oplus\boldsymbol{\beta}(a'))\mathbf{G}_1)+H((\boldsymbol{\beta}(a+\tau)\oplus\boldsymbol{\beta}(a'+\tau'))\mathbf{G}_2)\geq 3.$$

Using Theorem 1 it can be easily shown that $d_{1,min}(\boldsymbol{\pi})\geq 3$ and $d_{2,min}(\boldsymbol{\pi})\geq 3$, Therefore, it remains to prove that $H((\boldsymbol{\beta}(a)\oplus\boldsymbol{\beta}(a'))\mathbf{G}_1)$ and $H((\boldsymbol{\beta}(a+\tau)\oplus\boldsymbol{\beta}(a'+\tau'))\mathbf{G}_2)$ cannot be equal to 1 simultaneously.

For this let us first determine the set $\mathcal{W}\triangleq\{\mathbf{w}\in\mathbb{F}_2^R : H(\mathbf{w}\mathbf{G}_1)=1\}$. Clearly, $\mathcal{W}=\{\mathbf{w}_t, 1\leq t\leq R\}$, where $\mathbf{w}_t$ is the unique vector satisfying $\mathbf{w}_t\mathbf{G}_1=(\mathbf{0}_{t-1},1,\mathbf{0}_{R-t})$, $1\leq t\leq R$. It follows that

$$\mathbf{w}_t=(\mathbf{0}_{t-k-1},\mathbf{1}_{R-t+1},\mathbf{0}_k)\text{ for }k+1\leq t\leq R. \quad (9)$$

Additionally, one has

$$\mathbf{w}_t=(\mathbf{0}_{R-k+t-1},1,\mathbf{0}_{k-t})\oplus_{i=1}^{h}\mathbf{w}_{t_i+k})\text{ for }1\leq t\leq k,$$

where h denotes the Hamming weight of the t-th row of matrix $\mathbf{P}_1$, and $t_1,t_2,\cdots,t_h$ are the positions of the non-zero components of the t-th row of matrix $\mathbf{P}_1$, with $1\leq t_1<t_2<\cdots<t_h\leq R-k$. Property **C1** implies that h is odd, while **C3** leads to $t_1=1$ and $t_2=3$. Therefore, $\mathbf{w}_t$ becomes

$$\mathbf{w}_t=(11,\mathbf{0}_{t_3-3},\mathbf{1}_{R-k-t_3+1},\mathbf{0}_{t-1},1,\mathbf{0}_{k-t})\text{ for }h=3, \quad (10)$$

$$\mathbf{w}_t=(11,\mathbf{0}_{t_3-3},\mathbf{1}_{t_4-t_3},\cdots,\mathbf{0}_{t_h-t_{h-1}},\mathbf{1}_{R-k-t_h+1},\mathbf{0}_{t-1},1,\mathbf{0}_{k-t})\text{ for }h\geq 5. \quad (11)$$

To proceed with the proof let $\mathbf{u}\triangleq\boldsymbol{\beta}(a)\oplus\boldsymbol{\beta}(a')$ and $\mathbf{x}\triangleq\mathbf{u}\oplus\boldsymbol{\beta}(a+\tau)\oplus\boldsymbol{\beta}(a'+\tau')$. Next we will determine the form of vector $\mathbf{x}$. For this we will first analyze the form of $\boldsymbol{\beta}(a)\oplus\boldsymbol{\beta}(a+\tau)$. Let $a=c\times 2^k+e$, where $0\leq c\leq 2^{R-k}-1$, $0\leq e\leq 2^k-1$. Then $\boldsymbol{\beta}(a)=(\boldsymbol{\beta}_{R-k}(c),\boldsymbol{\beta}_k(e))$. Then for $a+\tau$ one of the following three situations is possible: **S1)** $0\leq e+\tau\leq 2^k-1$; **S2)** $-2^k\leq e+\tau\leq -1$; **S3)** $2^k\leq e+\tau\leq 2^{k+1}-1$.

If **S1** holds then $\boldsymbol{\beta}(a+\tau)=(\boldsymbol{\beta}_{R-k}(c),\boldsymbol{\beta}_k(e+\tau))$, leading to $\boldsymbol{\beta}(a)\oplus\boldsymbol{\beta}(a+\tau)=(\mathbf{0}_{R-k},\boldsymbol{\beta}_k(e)\oplus\boldsymbol{\beta}_k(e+\tau))$. In the case **S2** one has $\boldsymbol{\beta}(a+\tau)=(\boldsymbol{\beta}_{R-k}(c-1),\boldsymbol{\beta}_k(e+\tau+2^k))$. Let s denote the position of the rightmost 1 in $\boldsymbol{\beta}_{R-k}(c)$. Then $1\leq s\leq R-k$ and $\boldsymbol{\beta}_{R-k}(c-1)=\boldsymbol{\beta}_{R-k}(c)\oplus(\mathbf{0}_{s-1},\mathbf{1}_{R-k-s+1})$. Finally, in the case **S3** one has $\boldsymbol{\beta}(a+\tau)=(\boldsymbol{\beta}_{R-k}(c+1),\boldsymbol{\beta}_k(e+\tau-2^k))$. Then relation $\boldsymbol{\beta}_{R-k}(c+1)=\boldsymbol{\beta}_{R-k}(c)\oplus(\mathbf{0}_{s-1},\mathbf{1}_{R-k-s+1})$ holds, where s denotes the position of the rightmost 0 in $\boldsymbol{\beta}_{R-k}(c)$ (thus, $1\leq s\leq R-k$).

Further let $a'=c'\times 2^k+e'$ with $0\leq c'\leq 2^{R-k}-1$, $0\leq e'\leq 2^k-1$. For $i=1,2,3$ we say that $\mathbf{S}i$ holds for $a'+\tau'$ when the relations corresponding to $\mathbf{S}i$ are valid when e and τ are replaced by e' and τ', respectively. Combining now all possible cases for $a+\tau$ and for $a'+\tau'$ we obtain the following possible cases for $\mathbf{x}$.

X1) When **S1** holds for both $a+\tau$ and $a'+\tau'$ one has $\mathbf{x}_1^{R-k}=\mathbf{0}_{R-k}$.
X2) When a) **S1** holds for $a+\tau$ and either **S2** or **S3** holds for $a'+\tau'$; or b) **S1** holds for $a'+\tau'$ and either **S2** or **S3** holds for $a+\tau$, then $\mathbf{x}_1^{R-k}=(\mathbf{0}_{s-1},\mathbf{1}_{R-k-s+1})$ for

some $1 \leq s \leq R-k$.

X3) When either **S2** or **S3** holds for $a+\tau$ and either **S2** or **S3** holds for $a'+\tau'$ then $\mathbf{x}_1^{R-k} = \mathbf{0}_{R-k}$ or $\mathbf{x}_1^{R-k} = (\mathbf{0}_{s-1}, \mathbf{1}_{t-s}, \mathbf{0}_{R-k-t+1})$ for some $1 \leq s < t \leq R-k$.

To complete the proof we have to show that if $\mathbf{u} \in \mathcal{W}$ then $H(\mathbf{y}\mathbf{G}_2) > 1$, where $\mathbf{y} \triangleq \mathbf{u} \oplus \mathbf{x}$. From the form of matrix $\mathbf{G}_2$ it follows that

$$\mathbf{y}\mathbf{G}_2 = \mathbf{y}_1^{R-k-1}\mathbf{A}_2 \oplus \mathbf{y}_{R-k}^{R}\mathbf{B}_2. \tag{12}$$

Additionally, the fact that the number of 1's in the first $k+1$ positions of $\mathbf{y}\mathbf{G}_2$ equals $H(\mathbf{y}_{R-k}^R)$ implies that

$$H(\mathbf{y}\mathbf{G}_2) \geq H(\mathbf{y}_{R-k}^R). \tag{13}$$

Further, relation (12) together with the fact that $H(\mathbf{v}_1 \oplus \mathbf{v}_2) \geq |H(\mathbf{v}_1) - H(\mathbf{v}_2)|$, for any $\mathbf{v}_1, \mathbf{v}_2 \in \mathbb{F}_2^R$, lead to

$$H(\mathbf{y}\mathbf{G}_2) \geq |H(\mathbf{y}_1^{R-k-1}\mathbf{A}_2) - H(\mathbf{y}_{R-k}^R\mathbf{B}_2)|. \tag{14}$$

Assume now that $\mathbf{u} \in \mathcal{W}$. We need to consider two cases.

Case A1) $\mathbf{u} = \mathbf{w}_{k+t}$ for $1 \leq t \leq R-k$. Then relation (9) implies that $\mathbf{u} = (\mathbf{0}_{t-1}, \mathbf{1}_{R-k-t+1}, \mathbf{0}_k)$. Notice that $\mathbf{u}_{R-k+1}^R = \mathbf{0}_k$, which implies that $e = e'$. Next we need to consider three subcases.

Subcase A1.1) $\mathbf{x}_1^{R-k} = \mathbf{0}$. Then $\mathbf{y}_1^{R-k} = (\mathbf{0}_{t-1}, \mathbf{1}_{R-k-t+1})$. This implies that $y_{R-k} = 1$, yielding $\mathbf{y}_{R-k}^R\mathbf{B}_2 \geq d_{min}(\mathbf{B}_2) \geq 4$. Further, notice that when $t = R-k$ then $\mathbf{y}_1^{R-k-1}\mathbf{A}_2 = \mathbf{0}_R$, while for $t < R-k$ one has $\mathbf{y}_1^{R-k-1}\mathbf{A}_2 = (\mathbf{0}_{k+t}, 1, \mathbf{0}_{R-1-k-t})$. We conclude that $H(\mathbf{y}_1^{R-k-1}\mathbf{A}_2) \leq 1$. Applying now (14) one obtains that $H(\mathbf{y}\mathbf{G}_2) \geq 3$.

Subcase A1.2) $\mathbf{x}_1^{R-k} = (\mathbf{0}_{s-1}, \mathbf{1}_{R-k-s+1})$ for some $1 \leq s \leq R-k$. We will first show that

$$H(\mathbf{y}_1^{R-k-1}\mathbf{A}_2) \leq 2. \tag{15}$$

If $s = t$ then $\mathbf{y}_1^{R-k} = \mathbf{0}_{R-k}$, thus (15) holds. Consider now the case $s \neq t$. Assume without restricting the generality that $s < t$. Then one has $\mathbf{y}_1^{R-k-1} = (\mathbf{0}_{s-1}, \mathbf{1}_{t-s}, \mathbf{0}_{R-k-t})$ and (15) holds.

Next we will show that $\mathbf{y}_{R-k+1}^R \neq \mathbf{0}_k$. Recall that $e = e'$ and that **X2** holds. Assume that **S1** holds for $a+\tau$ and **S2** holds for $a'+\tau'$. Then $\mathbf{y}_{R-k+1}^R = \boldsymbol{\beta}_k(e) \oplus \boldsymbol{\beta}_k(e'+\tau'+2^k)$. Since $e'+\tau'+2^k > e' = e$ it follows that $\boldsymbol{\beta}_k(e) \oplus \boldsymbol{\beta}_k(e'+\tau'+2^k) \neq \mathbf{0}_k$ proving our claim. Assume now that **S1** holds for $a+\tau$ and **S3** holds for $a'+\tau'$. Then $\mathbf{y}_{R-k+1}^R = \boldsymbol{\beta}_k(e) \oplus \boldsymbol{\beta}_k(e'+\tau'-2^k) \neq \mathbf{0}_k$ since $e'+\tau'-2^k < e' = e$. The remaining cases of **X2** lead similarly to the desired conclusion.

The fact that $\mathbf{y}_{R-k+1}^R \neq \mathbf{0}_k$ implies that $H(\mathbf{y}_{R-k}^R\mathbf{B}_2) \geq d_{min}(\mathbf{B}_2)$. Corroborating with (15) and (14) one obtains that $H(\mathbf{y}\mathbf{G}_2) \geq 2$, thus completing the proof.

Subcase A1.3) $\mathbf{x}_1^{R-k} = (\mathbf{0}_{s-1}, \mathbf{1}_{q-s}, \mathbf{0}_{R-k-q+1})$ for some $1 \leq s < q \leq R-k$. If $t = s$ then $\mathbf{y}_1^{R-k} = (\mathbf{0}_{q-1}, \mathbf{1}_{R-k-q+1})$, while when $t = q$ we have $\mathbf{y}_1^{R-k} = (\mathbf{0}_{s-1}, \mathbf{1}_{R-k-s+1})$. Both these cases can be treated like **A1.1**.

Consider now the case $t < s$ (the discussions for $s < t < q$ and for $q < t$ are similar). Then $\mathbf{y}_1^{R-k} = (\mathbf{0}_{t-1}, \mathbf{1}_{s-t}, \mathbf{0}_{q-s}, \mathbf{1}_{R-k-q+1})$. Notice that $y_{R-k} = 1$. Therefore, $H(\mathbf{y}_{R-k}^R\mathbf{B}_2) \geq d_{min}(\mathbf{B}_2) \geq 4$. If $q = R-k$ then $H(\mathbf{y}_1^{R-k-1}\mathbf{A}_2) = 2$ and the claim follows via (14).

Now consider the case when $q < R-k$. We will first show that $\mathbf{y}_{R-k+1}^R \neq \mathbf{0}_k$. Notice that if **S2** held for both $a+\tau$ and $a'+\tau'$, the fact that $s, q < R-k$ would imply that both $\boldsymbol{\beta}_{R-k}(c)$ and $\boldsymbol{\beta}_{R-k}(c')$ end with a 0, thus contradicting the fact that $u_{R-k} = 1$. We conclude that **S2** cannot hold for both $a+\tau$ and $a'+\tau'$. It can be similarly shown that **S3** cannot hold for both $a+\tau$ and $a'+\tau'$. Therefore, since we are in the case **X3** we may assume without restricting the generality that **S2** holds for $a+\tau$ and **S3** holds for $a'+\tau'$. Then $\mathbf{y}_{R-k+1}^R = \boldsymbol{\beta}_k(e+\tau+2^k) \oplus \boldsymbol{\beta}_k(e'+\tau'-2^k)$. Since $e'+\tau'-2^k < e' = e < e+\tau+2^k$ it follows that $\mathbf{y}_{R-k+1}^R \neq \mathbf{0}_k$. Using further the fact that $y_{R-k} = 1$ it follows that $H(\mathbf{y}_{R-k}^R) \geq 2$ and the claim follows via (13).

Case A2) $\mathbf{u} = \mathbf{w}_t$ for $1 \leq t \leq k$. Then from (11) and (10) it follows that $\mathbf{u}_1^3 = (1,1,0)$ and $u_{R-k} = 1$. Examining all possibilities for $\mathbf{x}$ we conclude that $\mathbf{x}_1^3 \in \mathbb{F}_2^3 \setminus \{(1,0,1)\}$, which implies that $\mathbf{y}_1^3 = \mathbf{u}_1^3 \oplus \mathbf{x}_1^3 \in \mathbb{F}_2^3 \setminus \{(0,1,1)\}$. Denote now $\mathbf{z} \triangleq \mathbf{y}_1^{R-k-1}\mathbf{A}_2$. Then $\mathbf{z}_{k+2}^{k+4} \in \mathbb{F}_2^3 \setminus \{(0,1,0)\}$. Assume now that $H(\mathbf{y}_{R-k}^R) = 1$. Then property **C5** and (12) imply that $\mathbf{y}\mathbf{G}_2$ has the value 1 in at least one of the positions $k+2, k+3$ or $k+4$. Additionally, the vector $\mathbf{y}\mathbf{G}_2$ has one of the first $k+1$ components equal to 1, yielding $H(\mathbf{y}\mathbf{G}_2) \geq 2$.

By (13), it remains to discuss only the case when $\mathbf{y}_{R-k}^R = \mathbf{0}_k$. Then $\mathbf{y}\mathbf{G}_2 = \mathbf{z}$ and the non-trivial cases are when $H(\mathbf{z}_{k+2}^{k+4}) \leq 1$, i.e. when $\mathbf{x}_1^3 \in \{(1,1,0),(0,1,0),(1,0,0),(1,1,1)\}$. Further, notice that we have $y_{R-k} = 0$ and $u_{R-k} = 1$, implying that $x_{R-k} = 1$, which rules out case **X3**, therefore $\mathbf{x}_1^3 \notin \{(1,1,0),(0,1,0),(1,0,0)\}$. Now consider $\mathbf{x}_1^3 = (1,1,1)$. Then **X2** must hold with $s = 1$. Assume now that (10) holds. Then we have $\mathbf{y}_1^{R-k-1} = (0,0,\mathbf{1}_{t_3-3}, \mathbf{0}_{R-k-t_3})$. Note that by property **C2** relation $t_3 < R-k$ is valid implying that $H(\mathbf{z}) \geq 2$. The same conclusion follows when (11) holds, thus completing the proof of the theorem. ■

REFERENCES

[1] J. Barros, J. Hagenauer, N. Gortz, "Turbo cross decoding of multiple descriptions", *IEEE Int. Conf. Communic.*, 2002.

[2] I. Bahceci, Y. Altunbasak, and T. M. Duman, "A turbo-coded multiple-description system for multiple antennas", *IEEE Trans. Communic.*, vol. 54, pp. 187-191, Feb. 2006.

[3] R. Ma and F. Labeau, "Error-resilient multiple description coding", *IEEE Trans. on Signal Proc.*, vol. 56, pp. 3996-4007, Aug. 2008.

[4] Y. Zhou and W.-Y. Chan, "Multiple description quantizer design for multiple-antenna systems with MAP detection", *IEEE Trans. Communic.*, vol. 58, pp. 136-145, Jan. 2010.

[5] V. A. Vaishampayan, "Design of multiple-description scalar quantizers", *IEEE Trans. Inform. Th.*, vol. 39, no. 3, pp. 821-834, May 1993.

[6] T. Y. Berger-Wolf and E. M. Reingold, "Index Assignment for Multi-channel Communication Under Failure", *IEEE Trans. Inform. Th.*, vol. 48, no. 10, pp. 2656-2668, Oct. 2002.

[7] J. Balogh and J. A. Csirik, "Index assignment for two-channel quantization", *IEEE Trans. Inform. Th.*, vol. 50, no. 11, pp. 2737-2751, Nov. 2004.

[8] G. Zhang, J. Klejsa, W. B. Kleijn, "Optimal index assignment for multiple description scalar quantization with translated lattice codebooks", *IEEE Trans. Signal Proc.*, vol. 60, no. 8, pp. 4444 - 4451, Aug. 2012.

[9] R. W. Hamming, "Error detection and error correcting codes", *The Bell Syst. Tech. J.*, vol. 29, no. 2, pp. 147-160, Apr. 1950.