Error control of line codes generated by finite Coxeter groups

Ezio Biglieri
Universitat Pompeu Fabra, Barcelona, Spain
Email: e.biglieri@ieee.org

Emanuele Viterbo
Monash University, Melbourne, Australia
Email: emanuele.viterbo@monash.edu

Michele Elia
Politecnico di Torino, Italy
Email: michele.elia7@gmail.com

***Abstract*—A theory leading to the design of line group codes generated by Coxeter matrix groups was presented in [1]. With these codes, resistance to common-mode noise is obtained by using codewords whose components sum to zero, simultaneous switching output noise is reduced by using constant-energy signals, and the effects of intersymbol interference are reduced by having decisions based on only two values at the input of the final slicers. Codebook design is based on the theory of Group Codes for the Gaussian Channel [12], as specialized to Coxeter matrix groups generated by reflections in orthogonal hyperplanes. In this paper we discuss the introduction of error control coding in a way consistent with the constraints imposed on that design.**

I. Introduction and motivation of the work

In [1], we describe a general theory for the analysis and the design of a family of line codes for parallel transmission of b bits over $b+1$ wires that admit especially simple encoding and decoding algorithms. The resulting codebook is a geometrically uniform subset of a Permutation Modulation codebook [11]. With these codes, resistance to common-mode noise is obtained by using codewords whose components sum to zero, simultaneous switching output noise is reduced by using constant-energy signals, and the effects of intersymbol interference are reduced by having decisions based on only two values at the input of the final slicers [3], [4]. Codebook design is based on the theory of Group Codes for the Gaussian Channel [12], as specialized to Coxeter matrix groups generated by reflections in orthogonal hyperplanes.

The design procedure we advocate in [1] is based on the following steps:

① Pick an "initial" vector $\mathbf{w}_1$ whose $b+1$ real components sum to zero.

② Choose b "root" permutations $\mathbf{w}_2, \dots \mathbf{w}_{b+1}$ of $\mathbf{w}_1$ such that the b unit-norm vectors

$$\boldsymbol{\delta}_i \triangleq \frac{\mathbf{w}_1 - \mathbf{w}_{(i+1)}}{\|\mathbf{w}_1 - \mathbf{w}_{(i+1)}\|}, \qquad i = 1, \dots, b \tag{1}$$

are mutually orthogonal. An algorithm to do this is described in [1].

③ Compute the corresponding reflection matrices

$$\mathbf{O}_i \triangleq \mathbf{I} - 2\boldsymbol{\delta}_i\boldsymbol{\delta}_i^{\mathsf{T}} \tag{2}$$

Direct calculation shows that $\mathbf{O}_i^2 = (\mathbf{O}_i\mathbf{O}_j)^2 = \mathbf{I}$, so that these matrices are the generators of a Coxeter matrix group $\mathcal{G}$ isomorphic to a power of $\mathbb{Z}_2$. [2]

④ The code $\mathcal{W} = \mathcal{G}\mathbf{w}_1$ obtained by applying this matrix group to the initial vector $\mathbf{w}_1$ is a group code [12].

The wire efficiency of this code is $b/(b+1)$ bit/wire. If power consumption must be limited, one may want to exchange power efficiency for wire efficiency, that is, tolerate the use of a larger number of wires in exchange for power savings. This is similar in nature to the power vs. bandwidth tradeoff in wireless communication, which provides motivation to the introduction of error-control codes. Since the system described in [1] (see also [3]–[5]) is grounded on implementation simplicity, the employed coding schemes should allow coding/decoding with limited complexity. Some error-control coding (ECC) schemes were proposed in [5]. We describe in the following how the choice of a linear binary error-control code with rate ρ may increase the minimum Euclidean distance between words of the line codebook at the price of a decrease of its wire efficiency from $b/(b+1)$ to $\rho\, b/(b+1)$.

II. Theoretical foundations

Consider the information matrix $\mathbf{B}$ as defined in [1]. Its rows are all the $(b+1)$-tuples with entries in $\{\pm 1\}$ with a zero prepended. Removing the initial zero in each row, we are left with a $2^b \times b$ matrix with entries in $\{\pm 1\}$. The transformation from $\{\pm 1\}$ to $\{0, 1\}$ defined by $-1 \to 0$ and $+1 \to 1$ yields the new binary information matrix $\mathbf{C}$. The rows of $\mathbf{C}$, endowed with a componentwise mod-2 product, are the elements of a multiplicative group $\mathcal{C}$ isomorphic to $\mathbb{Z}_2^b$.

Further, consider the Coxeter matrix group $\mathcal{G}$ having as generators the matrices in the set $\{\mathbf{O}_i\}_{i=1}^b$ with relations $\mathbf{O}_i^2 = (\mathbf{O}_i\mathbf{O}_j)^2 = \mathbf{I}$. Every $\mathbf{G} \in \mathcal{G}$ can be written in the form of a product of matrices representing fundamental reflections, called its *expression*, $\mathbf{G} = \prod_{i=1}^b \mathbf{O}_i^{\varepsilon_i}$, with $\varepsilon_i \in \{0, 1\}$. This group is commutative and isomorphic to $\mathbb{Z}_2^b$.

Observation 1 *The map $\mu : \mathcal{C} \to \mathcal{G}$, defined as*

$$\mu(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_b) \triangleq \prod_{i=1}^{b} \mathbf{O}_i^{\varepsilon_i} \tag{3}$$

with $(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_b)$ a row of $\mathbf{C}$, is a group isomorphism. □

The application of the matrix group $\mathcal{G}$ to the initial vector $\mathbf{w}_1$ (assumed to have only the trivial stabilizer, i.e., to be left invariant only by the identity matrix) generates the codebook

$\mathcal{W}$ (the *orbit* of $\mathbf{w}_1$), whose 2^b words can be explicitly listed in the form of rows of a $2^b \times (b+1)$ matrix $\mathbf{W}$. The decision region of each word in the Euclidean space $\mathbb{R}^{b+1}$ is bounded by hyperplanes that are orthogonal to each other, which makes symbol-by-symbol detection to be maximum-likelihood in the presence of additive white Gaussian noise [1]. Consider next the set of Euclidean distances between $\mathbf{w}_1$ and the vectors of $\mathcal{W} = \mathcal{G}\mathbf{w}_1$, explicitly given by

$$d(\mathbf{G}) \triangleq \|\mathbf{G}\mathbf{w}_1 - \mathbf{w}_1\|, \qquad \mathbf{G} \in \mathcal{G} \tag{4}$$

(due to the properties of group codes [12], this set does not change if in lieu of $\mathbf{w}_1$ we use any vector in the orbit $\mathcal{G}\mathbf{w}_1$). In our context, linear ECC consists of choosing a subgroup $\mathcal{G}' \prec \mathcal{G}$ such that

$$\min_{\mathbf{G}' \in \mathcal{G}'} d(\mathbf{G}') > \min_{\mathbf{G} \in \mathcal{G}} d(\mathbf{G}) \tag{5}$$

In addition, we require the encoding and decoding operations to be sufficiently simple, and the rate loss $\rho = \log_2 |\mathcal{G}'| \,/\, |\mathcal{G}|$ be not too small.

A quantity useful to the description of our coding scheme is the *length* of an element of $\mathcal{G}$. The length of $\mathbf{G} = \prod_{i=1}^{g} \mathbf{O}_i^{\varepsilon_i}$ is defined as $\ell(\mathbf{G}) \triangleq \sum_{i=1}^{g} \varepsilon_i$. We have, for any generator matrix $\mathbf{O}_i$,

$$\ell(\mathbf{O}_i\mathbf{G}) = \begin{cases} \ell(\mathbf{G}) - 1, \text{if the expression of } \mathbf{G} \text{ contains } \mathbf{O}_i, \\ \ell(\mathbf{G}) + 1, \text{otherwise} \end{cases} \tag{6}$$

Thus, the maximum value of ℓ is b, achieved only for $\mathbf{G} = \prod_{i=1}^{b} \mathbf{O}_i$. Using the map of Observation 1, we can see that the length of $\mathbf{G}$ equals the Hamming weight of the row of $\mathbf{C}$ corresponding to $\mathbf{G}$, and hence of vector $\mathbf{G}\mathbf{w}_1$. In the Euclidean space $\mathbb{R}^{b+1}$ in which the codebook $\mathcal{W}$ is embedded, $\ell(\mathbf{G})$ is the number of reflection hyperplanes that have to be traversed to reach $\mathbf{G}\mathbf{w}_1$ from $\mathbf{w}_1$ [10].

We are especially interested in a possible proportionality between the length $\ell(\mathbf{G})$ and the distance $d(\mathbf{G})$, which leads to a correspondence between Hamming distances in a subgroup of $\mathcal{C}$ and Euclidean distances in the subgroup of $\mathcal{G}$ induced by the isomorphism (3). A direct connection between the Euclidean distance $d(\mathbf{G})$, $\mathbf{G} \in \mathcal{G}$, and the length $\ell(\mathbf{G})$ was observed in [10, Section VI] (see also [6]).

Before proceeding further, we derive an explicit expression of the mutual distances between pairs of vectors in $\mathcal{G}$. With $\mathbf{x}$ a real n-dimensional column vector, we observe that the squared Euclidean distance between $\mathbf{x}$ and $\mathbf{O}_i\mathbf{x}$ has the form

$$d^2(\mathbf{x}, \mathbf{O}_i\mathbf{x}) = (\mathbf{x} - \mathbf{O}_i\mathbf{x})^\mathsf{T}(\mathbf{x} - \mathbf{O}_i\mathbf{x}) = 2(\mathbf{x}^\mathsf{T}\mathbf{x} - \mathbf{x}^\mathsf{T}\mathbf{O}_i\mathbf{x}) \tag{7}$$

With $\mathbf{O}_i \triangleq \mathbf{I} - 2\boldsymbol{\delta}_i\boldsymbol{\delta}_i^\mathsf{T}$ as in (2), we obtain the compact expression for the Euclidean distance

$$d^2(\mathbf{x}, \mathbf{O}_i\mathbf{x}) = 2\big(\mathbf{x}^\mathsf{T}\mathbf{x} - \mathbf{x}^\mathsf{T}(\mathbf{I} - 2\boldsymbol{\delta}_i\boldsymbol{\delta}_i^\mathsf{T})\mathbf{x}\big) = 4(\mathbf{x}^\mathsf{T}\boldsymbol{\delta}_i)^2 \tag{8}$$

We have the following

Theorem 1 *The squared distances between $\mathbf{w}_1$ and the vectors in $\mathcal{G}\mathbf{w}_1$ have the form*

$$d^2\left(\mathbf{w}_1, \prod_{i=1}^{b} \mathbf{O}_i^{\varepsilon_i}\mathbf{w}_1\right) = 4\sum_{i=1}^{b} \varepsilon_i \left(\mathbf{w}_1^\mathsf{T}\boldsymbol{\delta}_i\right)^2 \tag{9}$$

To prove the above, observe that

$$(\mathbf{I} - 2\boldsymbol{\delta}_i\boldsymbol{\delta}_i^\mathsf{T})^{\varepsilon_i} = \mathbf{I} - 2\varepsilon_i\boldsymbol{\delta}_i\boldsymbol{\delta}_i^\mathsf{T} \qquad \forall i \tag{10}$$

Since the vectors $\boldsymbol{\delta}_i$ are mutually orthogonal and have unit norm, direct calculation proves (9). We also have the following:

Corollary 1 *The minimum d^2 of a Coxeter code is given by*

$$d^2_{\min} = 4\min_i(\mathbf{w}_1^\mathsf{T}\boldsymbol{\delta}_i)^2 \tag{11}$$

while the maximum d^2 is lower bounded by

$$d^2_{\max} \geqslant 4b\,\min_i(\mathbf{w}_1^\mathsf{T}\boldsymbol{\delta}_i)^2 \tag{12}$$

with equality in (12) *when the scalar products $\mathbf{w}_1^\mathsf{T}\boldsymbol{\delta}_i$ do not depend on i. This occurs when the polytope in $\mathbb{R}^{b+1}$ whose vertices are the tips of the codeword vectors is a hypercube (in this case we talk about* hypercube codes*).*

Now, consider error-control coding, obtained by choosing a subgroup $\mathcal{G}'$ of $\mathcal{G}$ as generated by restricting the rows of $\mathbf{C}$ to be the codewords of the linear binary algebraic code with length b, 2^k codewords, and minimum Hamming distance d_H. Denote by $\mathcal{L}_{b,k}$ the new Coxeter line code with length $b+1$ and dimension $k \leqslant b$. If d_k^2 denotes the minimum squared distance between any two codewords in $\mathcal{L}_{b,k}$, we have the following upper bound

$$d^2_{\min,\mathcal{G}'} \geqslant d^2_{\min} d_\mathrm{H} \tag{13}$$

From the above we may state the following:

Theorem 2 *If a Coxeter line code $\mathcal{L}_{b,b}$ is combined with a binary linear error-control code with parameters (b, k, d_H), its code rate (in terms of bits per wire) decreases from $b/(b+1)$ to $k/(b+1)$, while its minimum Euclidean distance increases from $d^2_{\min}$ to at least $d^2_{\min} d_\mathrm{H}$.*

and

Theorem 3 *If the scalar products $\mathbf{w}_1^\mathsf{T}\boldsymbol{\delta}_i$ do not depend on i, then we have*

$$d^2(\mathbf{w}_1, \mathbf{G}\mathbf{w}_1) = d^2_{\min}\ell(\mathbf{G}) \tag{14}$$

III. Code design

From Theorem 3, we see that for a hypercube code the square Euclidean distance between vertices $\mathbf{w}_1$ and $\mathbf{G}\mathbf{w}_1$ is proportional to the length $\ell(\mathbf{G})$, the number of reflections needed to reach $\mathbf{G}\mathbf{w}_1$ from $\mathbf{w}_1$:

$$d^2(\mathbf{w}_1, \mathbf{G}\mathbf{w}_1) = \kappa\,\ell(\mathbf{G}) \tag{15}$$

where κ is a positive constant. In these conditions, code design is tantamount to choosing a subgroup of the group $\mathcal{C}$ such that its vectors have a large Hamming weight, which is exactly the problem of selecting a linear binary code. This large weight translates into large lengths of the corresponding elements of $\mathcal{G}$, which in turn translates into large Euclidean distances among words of $\mathcal{G}'$.

Now, the conditions of Theorem 3 are not achieved whenever the line code is not a hypercube code. Thus, we are interested in deriving conditions which may hold for general codes. We examine two conditions weaker than (15):

$$\ell(\mathbf{G}_i) > \ell(\mathbf{G}_j) \Rightarrow \begin{cases} \|\mathbf{G}_i\mathbf{w}_1 - \mathbf{w}_1\|^2 > \|\mathbf{G}_j\mathbf{w}_1 - \mathbf{w}_1\|^2 & (\alpha) \\ \|\mathbf{G}_i\mathbf{w}_1 - \mathbf{w}_1\|^2 \geqslant \|\mathbf{G}_j\mathbf{w}_1 - \mathbf{w}_1\|^2 & (\beta) \end{cases} \tag{16}$$

We hasten to observe that neither (16)(α) nor (16)(β) necessarily hold, as shown in the example of Fig. 1.

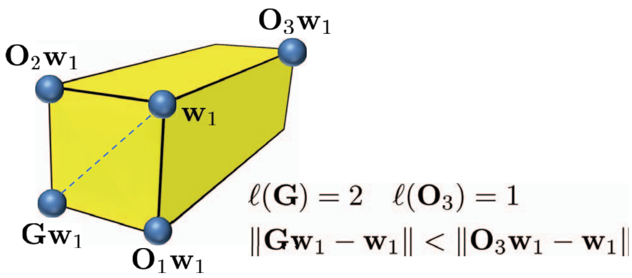

Fig. 1. *Part of a 3-dimensional codebook for which neither* (16)(α) *nor* (16)(β) *hold.*

Simple conditions for (16)(α) or (16)(β) to hold can be derived as follows. Consider the set $\mathcal{D}_\ell$ of squared distances from $\mathbf{w}_1$ to the words generated by group elements with length ℓ (the elements of $\mathcal{D}_\ell$ are the values taken on by the RHS of (9) when exactly ℓ of the ε_i are equal to 1). Define $\eta_i \triangleq 4(\mathbf{w}_1^\mathsf{T}\boldsymbol{\delta}_i)^2$, $i = 1, \dots, b$. Then (16)(α) holds if, for all ℓ, the largest element in $\mathcal{D}_\ell$ (i.e., the sum of the ℓ largest η_i) is smaller than the smallest element in $\mathcal{D}_{\ell+1}$ (i.e., the sum of the $\ell+1$ smallest η_i). Formally, we have the following result:

Theorem 4 *Define*

$$\eta_{(1)} \leqslant \cdots \leqslant \eta_{(b)} \tag{17}$$
$$\eta_{[1]} \geqslant \cdots \geqslant \eta_{[b]} \tag{18}$$

Then (16)(α) *is equivalent to*

$$\sum_{i=1}^{\ell} \eta_{[i]} < \sum_{i=1}^{\ell+1} \eta_{(i)}, \quad \ell = 1, \dots, b-1 \tag{19}$$

If at least one of the inequalities above is an equality, then (16)(β) *holds instead.*

A. Example 1

Consider $b = 2$, and the codebook generated by the matrix group whose generators are

$$\mathbf{O}_1 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \text{ and } \mathbf{O}_2 = \frac{1}{3}\begin{bmatrix} 2 & -1 & 2 \\ -1 & 2 & 2 \\ 2 & 2 & -1 \end{bmatrix} \tag{20}$$

The codebook, which we now organize into the matrix $\mathbf{W}$ whose rows are the codewords, is obtained as

$$\mathbf{W} = \begin{bmatrix} \mathbf{w}_1\mathbf{I} \\ \mathbf{w}_1\mathbf{O}_1 \\ \mathbf{w}_1\mathbf{O}_2 \\ \mathbf{w}_1\mathbf{O}_1\mathbf{O}_2 \end{bmatrix} \tag{21}$$

corresponding to the binary information matrix

$$\mathbf{C} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{bmatrix} \tag{22}$$

Choosing the initial vector $\mathbf{w}_1 = (-1, 0, 1)$, we obtain explicitly

$$\mathbf{W} = \begin{bmatrix} -1 & 0 & 1 \\ 0 & -1 & 1 \\ 0 & 1 & -1 \\ 1 & 0 & -1 \end{bmatrix} \tag{23}$$

Lengths and squared distances are shown in Table I. We see

TABLE I
Lengths and squared distances of codebook with $b = 2$.

length	squared-distance set
1	$\{2, 6\}$
2	$\{8\}$

that condition (16)(α) holds.

A simple error-control encoding scheme consists of selecting the following two rows of $\mathbf{C}$: $(0, 0)$ and $(1, 1)$ (repetition code). Geometrically, we end up with the subcode $(\mathbf{w}_1, \mathbf{w}_4)$ as generated by the matrix subgroup $\{\mathbf{I}, \mathbf{O}_1\mathbf{O}_2\}$ (see Fig. 2). Its minimum squared distance is 8.

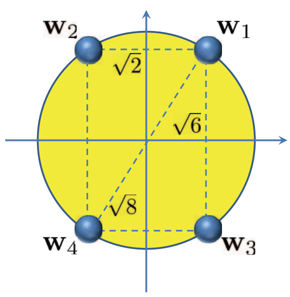

Fig. 2. *Code of Example 1.*

B. Example 2

With

$$\mathbf{C} = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \tag{24}$$

the matrices

$$\mathbf{O}_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$
$$\mathbf{O}_2 = \frac{1}{2}\begin{bmatrix} 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \\ -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \end{bmatrix} \tag{25}$$
$$\mathbf{O}_3 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

yield the codebook

$$\mathbf{W} = \begin{bmatrix} \mathbf{w}_1\mathbf{I} \\ \mathbf{w}_1\mathbf{O}_1 \\ \mathbf{w}_1\mathbf{O}_2 \\ \mathbf{w}_1\mathbf{O}_3 \\ \mathbf{w}_1\mathbf{O}_1\mathbf{O}_2 \\ \mathbf{w}_1\mathbf{O}_1\mathbf{O}_3 \\ \mathbf{w}_1\mathbf{O}_2\mathbf{O}_3 \\ \mathbf{w}_1\mathbf{O}_1\mathbf{O}_2\mathbf{O}_3 \end{bmatrix} \tag{26}$$

Choosing the initial vector $\mathbf{w}_1 = (-3, -1, 1, 3)$, we obtain explicitly

$$\mathbf{W} = \begin{bmatrix} -3 & -1 & 1 & 3 \\ -3 & 3 & 1 & -1 \\ -1 & -3 & 3 & 1 \\ 1 & -1 & -3 & 3 \\ -1 & 1 & 3 & -3 \\ 1 & 3 & -3 & -1 \\ 3 & -3 & -1 & 1 \\ 3 & 1 & -1 & -3 \end{bmatrix} \tag{27}$$

Lengths and squared distances are shown in Table II. We see that condition (16)(α) holds.

TABLE II
Lengths and squared distances of codebook with $b = 3$ and initial vector $\mathbf{w}_1 = (-3, -1, 1, 3)$.

length	squared-distance set
1	$\{16, 32\}$
2	$\{48, 64\}$
3	$\{80\}$

The choice of the initial vector $\mathbf{w}_1 = (-1, 0, 0, 1)$ yields a slightly different result, as shown in Table III. In this case the weaker condition (16)(β) holds.

TABLE III
Lengths and squared distances of codebook with $b = 3$ and initial vector $\mathbf{w}_1 = (-1, 0, 0, 1)$.

length	squared-distance set
1	$\{2, 4\}$
2	$\{4, 6\}$
3	$\{8\}$

The choice of the optimum initial vector for this matrix group, viz.,

$$\mathbf{w}_{1,\text{opt}} = \sum \frac{\mathbf{w}_1 - \mathbf{w}_i}{\|\mathbf{w}_1 - \mathbf{w}_i\|} \tag{28}$$

where the sum runs through the set of root permutations [1], [9], yields a codebook whose components are not integer numbers (they take values $\pm 1/2 \pm 1/\sqrt{2}$) and yield the results summarized in Table IV. In this case the resulting constellation has a shape of a 3-dimensional cube, and the stronger condition (15) holds. In fact:

$$\|\mathbf{G}\mathbf{w}_1 - \mathbf{w}_1\|^2 = 4\ell(\mathbf{G}) \tag{29}$$

TABLE IV
Lengths and squared distances of codebook with $b = 3$ and optimum initial vector (28).

length	squared-distance set
1	$\{4\}$
2	$\{8\}$
3	$\{12\}$

To error-control encode any of these three line codebooks, we select the rows of $\mathbf{C}$ having an even number of 1s (single-parity-check code). Geometrically, we end up with the subcode $(\mathbf{w}_1, \mathbf{w}_5, \mathbf{w}_6, \mathbf{w}_7)$ generated by the matrix subgroup $\{\mathbf{I}, \mathbf{O}_1\mathbf{O}_2, \mathbf{O}_1\mathbf{O}_3, \mathbf{O}_2\mathbf{O}_3\}$ (see Fig. 3).[1] With this choice, the minimum squared distance of the error-control-coded codebook increases from 16 to 48 with the choice $\mathbf{w}_1 = (-3, -1, 1, 3)$, from 2 to 4 with the choice $\mathbf{w}_1 = (-1, 0, 0, 1)$, and from 4 to 8 with the optimum choice of $\mathbf{w}_1$.

C. Example 3

With $b = 4$, and the codebook in [1, Table 3] with initial vector $\mathbf{w}_1 = (-2, -1, 0, 1, 2)$, we have the situation summarized in Table V.

[1] Observe that this subgroup is not a Coxeter group, as it is not generated by reflections. In fact, $\mathbf{O}_1\mathbf{O}_2$ and $\mathbf{O}_2\mathbf{O}_3$ do not have determinants equal to -1.

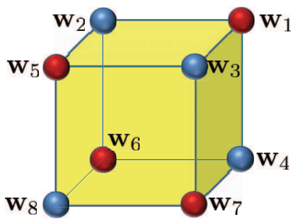

Fig. 3. *Code of Example 2.*

TABLE V
Lengths and squared distances of codebook with $b = 4$ *in [1, Table 3] with initial vector* $\mathbf{w}_1 = (-2, -1, 0, 1, 2)$.

length	squared-distance set
1	$\{4, 8, 20\}$
2	$\{12, 16, 24, 28\}$
3	$\{20, 32, 36\}$
4	$\{40\}$

With the same construction of the matrix group as in [1, Table 3], with an initial vector close to the optimum one but with integer entries, i.e., $\mathbf{w}_1 = (-7, -2, 0, 5, 4)$, we obtain the results summarized in Table VI.

TABLE VI
Lengths and squared distances of codebook with $b = 4$ *in [1, Table 3], but with initial vector* $\mathbf{w}_1 = (-7, -2, 0, 5, 4)$.

length	squared-distance set
1	$\{80, 100\}$
2	$\{180, 200\}$
3	$\{280, 300\}$
4	$\{380\}$

We can see that the codebook of Table VI, generated by an initial vector close to the optimum one, has squared distances satisfying the approximate condition

$$\|\mathbf{G}\mathbf{w}_1 - \mathbf{w}_1\|^2 \cong 100\,\ell(\mathbf{G}) \tag{30}$$

while that of Table V does not even satisfy the weak condition (16)(β).

D. Example 4

Choose $b = 5$, and the codebook described in [1, Example 6] with initial vector $\mathbf{w}_1 = (1, -1, 3, -3, 5, -5)$. We have the situation summarized in Table VII. One can see that neither (16)(α) nor (16)(β) hold in this case. Nonetheless, the use of a single-parity-check code, selecting words corresponding to the group elements with $\ell = 0, 2$, and 4, the minimum distance of the error-control-coded codebook increases from 8 to 16. Selecting an initial vector closer to the optimum one, viz., $\mathbf{w}_1 = (1, -1, 2, -2, 7, -7)$, we obtain a codebook whose geometric representation is closer to a hypercube, and the distance set are as in Table VIII. We see that the distance spectra satisfy (16)(α), and, approximately, condition (15) with $\kappa \cong 90$. Again, the use of a single-parity-check code, which reduces the wire efficiency (from $5/6$ to $4/6$), doubles the minimum square distance (from 72 to 144).

TABLE VII
Lengths and squared distances of codebook with $b = 5$ *in [1, Table 3], with initial vector* $(1, -1, 3, -3, 5, -5)$.

length	squared-distance set
1	$\{8, 24\}$
2	$\{16, 32, 48\}$
3	$\{40, 56, 72\}$
4	$\{64, 80\}$
5	$\{88\}$

TABLE VIII
Lengths and squared distances of codebook with $b = 5$ *in [1, Table 3], with initial vector* $(1, -1, 2, -2, 7, -7)$.

length	squared-distance set
1	$\{72, 94\}$
2	$\{144, 168, 192\}$
3	$\{240, 264, 288\}$
4	$\{336, 360\}$
5	$\{432\}$

IV. Using Reed-Muller codes

In addition to single-parity-check codes, a rather natural choice for the selection of an error-control code admitting simple soft decoding can be found in the framework of first-order Reed–Muller codes [7], [8]. These codes do not have an especially high rate, but decoding is relatively simple. The following properties hold: For any $m > 0$, the first-order Reed–Muller code $\mathcal{R}(1, m)$ is a binary linear code with length 2^m, 2^{m+1} codewords (and hence rate $(m + 1)/2^m$), and minimum Hamming distance 2^{m-1}. In particular, every codeword, except the all-0 and the all-1 codewords, has Hamming weight 2^{m-1}.

For example, the Reed-Muller code $\mathcal{R}(1, 2)$ is a single-parity-check code, whose use was mentioned in Example 3 above. Another code which might come in handy is $\mathcal{R}(1, 3)$, which has 2^4 binary words of length 8, rate $1/2$, and minimum Hamming weight 4. This may be used with a line code having $b = 8$, and would reduce the wire efficiency from $8/9$ to $4/9$.

Acknowledgment

The work of Ezio Biglieri is supported by Project TEC2015-66228-P. The work of Emanuele Viterbo is supported by ARC under Grant Discovery Project No. DP160101077.

References

[1] E. Biglieri and E. Viterbo, "Line codes generated by finite Coxeter groups," *Submitted for publication*, 2017. [Cited on p. 1, 2, 4, 5]

[2] H. S. M. Coxeter, "Discrete groups generated by reflections," *Annals of Mathematics*, vol. 35, no. 3, pp. 588–621, July 1934. [Cited on p. 1]

[3] "A primer on chord signaling," Downloaded August 2016 from website https://www.kandou.com/technology/coding. [Cited on p. 1]

[4] H. Cronie and A. Shokrollahi, "Orthogonal differential vector signaling," Patent Application US 2011/0268225 A1, November 3, 2011. [Cited on p. 1]

[5] H. Cronie and A. Shokrollahi, "Error control coding for orthogonal differential vector signaling," US Patent 2011/0299555 A1, December 8, 2011. [Cited on p. 1]

[6] J. E. Humphreys, *Reflection Groups and Coxeter Groups*. Cambridge, U.K.: Cambridge Univ. Press, 1985. [Cited on p. 2]

[7] S. Lin and D. J. Costello, Jr., *Error Control Coding*. Upper Saddle River, NJ: Pearson Prentice Hall, 2004. [Cited on p. 5]

[8] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: Elsevier, 1988. [Cited on p. 5]

[9] T. Mittelholzer and J. Lahtonen, "Group codes generated by finite reflection groups," *IEEE Trans. Inform. Theory*, vol. 42, no. 2, pp. 519–528, March 1996. [Cited on p. 4]

[10] W. W. Peterson, J. B. Nation, and M. P. Fossorier, "Reflection group codes and their decoding," vol. 56, no. 12, pp. 6273–6293, December 2010. [Cited on p. 2]

[11] D. Slepian, "Permutation modulation," *IEEE Proceedings*, pp. 228–236, March 1965. [Cited on p. 1]

[12] D. Slepian, "Group codes for the Gaussian channel," *Bell System Technical Journal*, vol. 47, pp. 575–602, 1968. [Cited on p. 1, 2]