Orthogonal designs and a cubic binary function

Sophie Morier-Genoud, Valentin Ovsienko

Orthogonal Designs and a Cubic Binary Function

Sophie Morier-Genoud Valentin Ovsienko

Abstract—**Orthogonal designs are fundamental mathematical notions used in the construction of space time block codes for wireless transmissions. Designs have two important parameters, the rate and the decoding delay; the main problem of the theory is to construct designs maximizing the rate and minimizing the decoding delay.**

All known constructions of CODs are inductive or algorithmic. In this paper, we present an explicit construction of optimal CODs. We do not apply recurrent procedures and do calculate the matrix elements directly. Our formula is based on a cubic function in two binary n-vectors. In our previous work (Comm. Math. Phys., 2010, and J. Pure and Appl. Algebra, 2011), we used this function to define a series of non-associative algebras generalizing the classical algebra of octonions and to obtain sum of squares identities of Hurwitz-Radon type.

Index Terms—**Orthogonal designs, decoding delay, maximal rate, peak-to-average power ratio, space-time codes, generalized octonions.**

I. INTRODUCTION

Orthogonal designs first appeared in the classical work of Hurwitz [13], [14] and Radon [17], in order to solve the problem of sum of squares identities (also known as composition of quadratic forms). This problem can be formulated in different ways and related to many mathematical questions (normed division algebras, vector fields on spheres, Clifford modules, immersion of projective spaces in euclidean spaces...) arising in different fields. The general problem is widely open and keep inspiring work of many mathematicians, see [18] and [20] for surveys. In the 1970's, orthogonal designs and their generalizations have been extensively studied from combinatorial and number theoretic viewpoints, see Geramita et al. [6]–[9] and references therein.

Orthogonal designs keep attracting much attention, since they are used to construct space-time block codes for wireless communication with multiple transmit antennas. This idea was introduced by Tarokh, Jafarkhani and Calderbank [12], as a generalization of the Alamouti scheme [3] for wireless communication with two antennas. Space-time block codes built out of the orthogonal designs achieve full transmit diversity and have a simple maximum likelihood decoding algorithm.

In this paper, we describe a method of construction of orthogonal designs. Unlike all known constructions which are inductive, i.e., use block matrices of small sizes to construct bigger matrices, our construction calculates elements of the matrices directly. In particular, we construct designs satisfying optimal criteria of [10] and [1], [2]. We also construct designs of type [12] and [5] defined by matrices that have no zero elements.

S. Morier-Genoud, Université Paris 6, IMJ, UFR 929 de Mathématiques, Case 247, 4 pl. Jussieu, 75005 Paris, France; sophiemg@math.jussieu.fr

V. Ovsienko, CNRS, ICJ, Université Lyon 1, 43 bd. du 11 novembre 1918, 69622 Villeurbanne cedex, France; ovsienko@math.univ-lyon1.fr

A. Definitions and known results

Definition 1: A *real orthogonal design* (ROD) of type $[p, n, k]$ is a matrix G of size $p \times n$ with real entries $0, \pm x_1, \cdots, \pm x_k$, satisfying

$$G^T G = \left(x_1^2 + \cdots + x_k^2\right) I_n,$$

where G^T is the transpose matrix of G.

Definition 2: A *complex orthogonal design* (COD) of parameters $[p, n, k]$ is a matrix H of size $p \times n$ with complex entries $0, \pm z_1, \cdots, \pm z_k$, and their conjugates $\pm z_1^*, \cdots, \pm z_k^*$, satisfying

$$H^* H = \left(|z_1|^2 + \cdots + |z_k|^2\right) I_n,$$

where H^* is the complex conjugate transpose of H.

Definition 3: Given a $[p, n, k]$-(R or C)OD, the ratio $\frac{k}{p}$ is called the *rate* of the design and the parameter p is called the *decoding delay* of the design.

The main problem in the construction of real or complex orthogonal designs is to maximize the rate $\frac{k}{p}$ and minimize the delay p for a given n. The following answers have been provided

1) $[p, n, k]$-ROD of rate 1 exist for all n, and in this case the minimum delay is $p = 2^{\delta(n)}$, where

$$\delta(n) = \begin{cases} \frac{n}{2} & \text{if } n = 2, 4, 6 \mod 8\ , \\ \frac{n-1}{2} & \text{if } n = 1, 7 \mod 8\ , \\ \frac{n+1}{2} & \text{if } n = 3, 5 \mod 8\ , \\ \frac{n}{2} - 1 & \text{if } n = 0 \mod 8. \end{cases}$$

This is a way to formulate the classical theorem or Hurwitz and Radon.

2) Using a doubling process of ROD of rate 1, Tarokh et al. [12] obtain COD of rate $\frac{1}{2}$ and decoding delay $2^{\delta(n)+1}$; We will denote by $\mathbf{TJC}_n$ this class of CODs, the parameters are

$$\left[2^{\delta(n)+1}, n, 2^{\delta(n)}\right].$$

3) Liang [10] proves that the maximal rate of a $[p, n, k]$-COD with $n \neq p$ is $\frac{1}{2} + \frac{1}{n}$, if n is even, and $\frac{1}{2} + \frac{1}{n+1}$, if n is odd.

4) Adams et al. [1] and [2] find a tight lower bound for the decoding delay p in a non-square COD achieving the maximal rate given by a binomial coefficient. Let $n = 2m - 1$ or $n = 2m$, then

$$p \geq \binom{2m}{m-1},$$

for $n = 0, 1, 3 \mod 4$ and

$$p \geq 2\binom{2m}{m-1},$$

for $n = 2 \mod 4$. We will denote by $\mathbf{LA}_n$ the class of CODs achieving the maximal rate and minimal decoding delay.

5) Liang [10] and Lu et al. [11] give algorithms to produce designs of type $\mathbf{LA}_n$. Another construction is given in [4].
6) Das and Rajan [5] construct CODs of rate $\frac{1}{2}$ and decoding delay $2^{\delta(n)}$. We will denote by $\mathbf{DR}_n$ this class of CODs, the parameters are

$$\left[2^{\delta(n)},\, n,\, 2^{\delta(n)-1}\right].$$

It is interesting that the decoding delay of these CODs is twice lower than that of $\mathbf{TJC}_n$.

Let us stress that CODs of rate $\frac{1}{2}$ are of interest, since for large values of n the maximal rate is almost $\frac{1}{2}$. For instance, for $n = 12$ the COD $\mathbf{LA}_n$ has rate $\frac{7}{12}$ and decoding delay 792, whereas $\mathbf{DR}_n$ has rate $\frac{1}{2}$ and decoding delay 64, see [5] for a comparative table.

B. Main results and organization of the paper

The goal of this article is to present a unified construction of RODs and CODs.

We start with an explicit formulas for the matrices G of size $2^r \times 2^r$ satisfying the conditions of ROD. The rows and columns of the matrices are labelled by elements in the set $\mathbb{Z}_2^r$, i.e., of r-vectors with coefficients 0 and 1. The entries in the matrices are given by an explicit function $f : \mathbb{Z}_2^r \times \mathbb{Z}_2^r \to \mathbb{Z}_2$. We then explain an easy way to reduce a RODs to a CODs.

With our method we construct RODs with parameters:

- $\left[2^{\delta(2r)},\, 2r,\, 2^{\delta(2r)}\right]$,
that will produce CODs with same parameters as $\mathbf{TJC}_n$ (using a doubling process) and with same parameters as $\mathbf{DR}_n$ (using a reduction process), provided $n \neq 1 \mod 8$;
- $\left[2\binom{r+1}{m-1},\, 2r,\, 2\binom{r}{m}\right]$, if $r = 0, 1, 3 \mod 4$,

  $\left[4\binom{r+1}{m-1},\, 2r,\, 2\binom{r}{m}\right]$, if $r = 0 \mod 4$,

  where m is defined by $r = 2m - 1$ or $2m$. These RODs will reduce to COD with same parameters as $\mathbf{LA}_n$.

The paper is organized as follows. The next section contains the main ingredients of our approach. We construct RODs with parameters that are twice the parameters of the optimal CODs.

Section III describes the reduction from the $[p, n, k]$-RODs to $\left[\frac{p}{2},\, \frac{n}{2},\, \frac{k}{2}\right]$-CODs, leading to optimal CODs of type $\mathbf{LA}_n$.

Section IV presents a procedure that allows us to construct a $\left[\frac{p}{2},\, n,\, k\right]$-COD out of a $[p, n, k]$-ROD, provided the ROD is stable under the duality. We thus obtain the CODs of types $\mathbf{TJC}_n$ and $\mathbf{DR}_n$. Let us mention that the corresponding matrices have no zero entries.

Proofs of technical statements, as well as properties of the binary functions we use, are collected in Appendix.

II. General construction of RODs

A. Combinatorics over $\mathbb{Z}_2$

We denote by $\mathbb{Z}_2^r$ the set of r-vectors $u = (u_1, \ldots, u_r)$, where $u_i = 0$ or 1[1]. The *Hamming weight* $|u|$ of an element is the number of non-zero component, i.e.

$$|u| = \#\left\{u_i = 1\right\}_{1 \leq i \leq r}.$$

The sum of two elements u and v is just the sum componentwise modulo 2. Every element is a sum of the basis vectors

$$\varepsilon^j = (0, \ldots, 0, 1, 0, \ldots, 0),$$

with 1 at j-th position. We will also consider the element of maximal weight r:

$$\varepsilon = (1, 1, \ldots, 1).$$

We will use the involution on $\mathbb{Z}_2^r$, that we call the "hat duality":

$$\hat{u} = u + \varepsilon^1, \tag{1}$$

i.e., the change of 1st coordinate.

The following function in two arguments $f : \mathbb{Z}_2^r \times \mathbb{Z}_2^r \to \mathbb{Z}_2$ plays the key rôle in our approach:

$$\boxed{f(u,v) = \sum_{i<j<k} (u_i u_j v_k + u_i v_j u_k + v_i u_j u_k) + \sum_{i \leq j} u_i v_j,}$$

We will also use the function in one variable $\alpha(u) := f(u, u)$, given explicitly by

$$\alpha(u) = \sum_{i<j<k} u_i u_j u_k + \sum_{i \leq j} u_i u_j.$$

The value of $\alpha(u)$ depends only on the weight of u:

$$\alpha(u) = \begin{cases} 0 & \text{if } |u| = 0 \mod 4, \\ 1, & \text{otherwise.} \end{cases}$$

The function f is used in all the constructions to determine signs, while α is used as a "statistic" to select good elements of $\mathbb{Z}_2^r$. Properties of f and α are presented in Appendix.

B. General construction of RODs

In this section, we construct $(p \times n)$-matrices whose rows and columns are indexed by subsets $W \subset \mathbb{Z}_2^r$ and $V \subset \mathbb{Z}_2^r$ of cardinality p and n, respectively.

We define the matrix G_u, $u \in \mathbb{Z}_2^r$ by

$$G_u = \begin{array}{cc} \begin{array}{c} v \end{array} & \\ \left(\begin{array}{ccc} & \vdots & \\ & \vdots & \\ \cdots & G_u^{w,v} & \cdots \\ & \vdots & \end{array} \right) & \begin{array}{c} \\ \\ w \\ \\ \end{array} \end{array}$$

where the entry in position (w, v) is

$$G_u^{w,v} = \begin{cases} (-1)^{f(u,v)}, & \text{if } u = v + w, \\ 0, & \text{otherwise.} \end{cases}$$

[1]We use the notation $\mathbb{Z}_2 = \{0, 1\}$ for the abelian group of rank 2, other notations: $\mathbb{F}_2$ and $\mathbb{Z}/2\mathbb{Z}$ are also often used.

The following properties are obvious:

1) the matrix G_u has at most one nonzero element on each row and on each column;
2) if $V = W = \mathbb{Z}_2^r$, then G_u is a $(2^r \times 2^r)$-matrix with exactly one non-zero element on each row and column.

Definition 4: We call U, V, W an *admissible triple* if the following two conditions are satisfied:

1)
$$W = U + V,$$
i.e., $u + v \in W$ for all $u \in U$ and $v \in V$ and every element $w \in W$ can be written in the form $w = u + v$.
2) If a non-zero element $w \in W$ decomposes in two ways: $w = u + v = u' + v'$ then
$$\alpha(u + u') = \alpha(v + v') = 1. \tag{2}$$

Theorem 1: If U, V, W is an admissible triple, then one has:
(i) $G_u^T G_u = I_n$, for all $u \in U$.
(ii) $G_u^T G_{u'} + G_{u'}^T G_u = 0$, for all $u \neq u' \in U$.

This theorem is proved in [16] and [15]. For the sake of completeness, we include the proof into Appendix.

Corollary 1: If U, V, W is an admissible triple, then
(i) the matrix
$$G = \sum_{u \in U} x_u G_u$$
is a ROD with parameters $[\#W, \#V, \#U]$ in real variables x_u, $u \in U$, where $\#$ is the cardinality of a set;
(ii) in the case of rate 1, i.e., where $k = p$, the matrix G has *no zero entries*.

Our next task is to construct admissible triples U, V, W. We will use the fact that the function α vanishes only on the elements whose weight is a multiple of 4. Note that the easiest way to guarantee condition (2) is to choose the set V so that $\alpha(v + v') = 1$ for all $v, v' \in V$.

C. RODs of rate 1

In this section, we provide triples of sets U, V, W that produce real orthogonal designs
$$G = \sum_{u \in U} x_u G_u$$
of rate 1, with minimum delay, i.e. the parameters of G are $\left[2^{\delta(n)}, n, 2^{\delta(n)}\right]$, (provided $n \neq 1 \mod 8$).

Case $r = 0, 1, 2 \mod 4$. One chooses the following subsets
$$\begin{aligned} V &= \left\{\varepsilon^j, \widehat{\varepsilon^j}, 1 \leq j \leq r\right\}, \\ U &= W = \mathbb{Z}_2^r, \end{aligned}$$
where $\hat{}$ is the duality (1). Then G is a $[2^r, 2r, 2^r]$-ROD. [2]

[2]This ROD is optimal, except for the case $r = 0 \mod 4$, where, according to the Hurwitz-Radon theorem, there is a $[2^r, 2r + 1, 2^r]$-ROD. We do not dwell here on a more involved construction to produce such a ROD.

Case $r = 3 \mod 4$. One chooses the following subsets
$$\begin{aligned} V &= \left\{\varepsilon, \widehat{\varepsilon}, \varepsilon^j, \widehat{\varepsilon^j}, 1 \leq j \leq r\right\}, \\ U &= W = \mathbb{Z}_2^r, \end{aligned}$$
the G is a $[2^r, 2r + 2, 2^r]$-ROD.

D. Non-square RODs of rate $\frac{1}{2} + \frac{1}{2m}$

All the RODs below have maximal rate $\frac{1}{2} + \frac{1}{2m}$, when $r = 2m$ or $2m - 1$.

Case $r = 1, 2 \mod 4$. Consider $r = 2m - 1$ or $r = 2m$ and choose the set U of the elements of weight m and their dual, the set V is chosen as in the first case:
$$\begin{aligned} U &= \{u, \hat{u} : |u| = m\}, \\ V &= \left\{\varepsilon^j, \widehat{\varepsilon^j}, 1 \leq j \leq r\right\}, \end{aligned}$$
It follows that the space $W = U + V$ is:
$$\begin{aligned} W = \; & \{u : |u| = m - 1, m, m + 1\} \bigcup \\ & \{u : u_1 = 1, |u| = m + 2\} \bigcup \\ & \{u : u_1 = 0, |u| = m - 2\}. \end{aligned}$$
The matrix G is a ROD with parameters
$$\left[2\binom{r+1}{m-1}, 2r, 2\binom{r}{m}\right], \quad \left[4\binom{r}{m-1}, 2r, 2\binom{r}{m}\right],$$
for odd r and even r, respectively.

Case $r = 0 \mod 4$. Consider $r = 2m$ (where m is even) and choose the following subsets
$$\begin{aligned} U &= \{u : u_1 = 1, |u| = m\} \bigcup \\ & \quad \{u : u_1 = 0, |u| = m - 1\}, \\ V &= \left\{\varepsilon, \hat{\varepsilon}, \varepsilon^j, \widehat{\varepsilon^j}, 2 \leq j \leq n\right\}, \\ W &= \{u : u_1 = 1, |u| = m - 1, m + 1\} \bigcup \\ & \quad \{u : u_1 = 0, |u| = m - 2, m\}, \end{aligned}$$
then G is a $\left[2\binom{r}{m-1}, 2r, 2\binom{r-1}{m-1}\right]$-ROD.

Case $r = 3 \mod 4$. Consider $r' := r + 1$ and apply the previous case with $r' = 0 \mod 4$ to obtain a $\left[2\binom{r+1}{m-1}, 2r + 2, 2\binom{r}{m}\right]$-ROD, where $r = 2m - 1$. Removing two columns, we obtain a $\left[2\binom{r+1}{m-1}, 2r, 2\binom{r}{m}\right]$-ROD.

In each of the above cases, condition (2) is satisfied for all $v, v' \in V$.

To finish this section, let us mention that the binary numeration have already been efficiently used in [4], [5] to construct RODs and CODs of maximal rate. In particular, subsets of $\mathbb{Z}_2^r$ similar to our sets U, V and W were described. The main difference of our approach is the function f and explicit construction of the matrices.

III. Reduction from ROD to COD

In this section, we present a procedure to reduce a $[2p, 2n, 2k]$-ROD to a $[p, n, k]$-COD. Such a procedure is not always possible, it requires nice properties of sets U, V, W. We first describe the general procedure of reduction and then apply it to RODs of rate 1 constructed in Section II-C.

A. The general procedure

The main idea is to use a duality

$$\widehat{\ }: \mathbb{Z}_2^r \to \mathbb{Z}_2^r$$

defined by $\hat{u} = u + e$, where the element $e \in \mathbb{Z}_2^r$ satisfies $f(e, e) = 1$, and to choose sets U, V and W stable under the duality:

$$\widehat{U} = U, \quad \widehat{V} = V, \quad \widehat{W} = W,$$

In practice, we use the hat duality (1), i.e., $e = \varepsilon^1$.

Given a ROD of type $[2p, 2n, 2k]$ defined by sets U, V and W in $\mathbb{Z}_2^r$, our goal is to reduce it to a COD with parameters $[p, n, k]$. The method consists in two steps. First, we introduce splitting of the sets U, V, W, in order to decompose the matrices $G = \sum_{u \in U} x_u G_u$ into admissible (2×2)-blocks. Second, we replace the admissible blocks by complex variables, $z_u = x_u + i x_{\hat{u}}$ or $z_u^* = x_u - i x_{\hat{u}}$.

STEP 1: We fix the following splitting of U

$$\begin{aligned} U_0 &:= \{u \in U : f(u, e) = 0\}, \\ U_1 &:= \{u \in U : f(u, e) = 1\}. \end{aligned} \tag{3}$$

Note that $\widehat{U_0} = U_1$, cf. Property (b) of f in Appendix.

We now need to find subsets V_0, V_1, W_0 and W_1 satisfying the following conditions

$$\begin{array}{rclcl} V &=& V_0 \bigsqcup V_1, && V_1 = \widehat{V_0}; \\ W &=& W_0 \bigsqcup W_1, && W_1 = \widehat{W_0}; \\ W_0 &=& U_0 + V_0 &=& U_1 + V_1; \\ W_1 &=& U_0 + V_1 &=& U_1 + V_0, \end{array} \tag{4}$$

where $\bigsqcup$ denotes the disjoint union.

These splitting induce a natural decomposition of the matrices G_u into (2×2)-blocks whose columns are labelled by $(v, \hat{v}) \in V_0 \times V_1$ and the rows by $(w, \hat{w}) \in W_0 \times W_1$:

$$G_u = \begin{array}{c} \begin{array}{cc} v & \hat{v} \end{array} \\ \left(\begin{array}{ccc} & \vdots \ \vdots & \\ & \vdots \ \vdots & \\ \cdots & \boxed{\widetilde{G}_u^{w,v}} & \cdots \\ & \vdots \ \vdots & \end{array} \right) \end{array} \begin{array}{c} \\ \\ w \\ \hat{w} \\ \\ \end{array}$$

where $u = v + w$ and so $\hat{u} = v + \hat{w} = \hat{v} + w$.

For $u \in U_0$ (and therefore $\hat{u} \in U_1$), the non-zero blocks are of the form

$$\widetilde{G}_u^{w,v} = \begin{pmatrix} (-1)^{f(u,v)} & 0 \\ 0 & (-1)^{f(u,\hat{v})} \end{pmatrix}$$

and

$$\widetilde{G}_{\hat{u}}^{w,v} = \begin{pmatrix} 0 & (-1)^{f(\hat{u},v)} \\ (-1)^{f(\hat{u},\hat{v})} & 0 \end{pmatrix};$$

non-zero blocks are located at the same place in G_u and $G_{\hat{u}}$.

Moreover, since f is linear in the 2nd variable,

$$\begin{aligned} f(u, \hat{v}) &= f(u, v) + f(u, e) &= f(u, v), \\ f(\hat{u}, \hat{v}) &= f(\hat{u}, v) + f(\hat{u}, e) &= f(\hat{u}, v) + 1, \end{aligned}$$

so that the entries in the blocks of G_u are of the same sign and those of $G_{\hat{u}}$ are of the opposite sign.

STEP 2: The matrix $G = \sum_{u \in U} x_u G_u$ decomposes into (2×2)-blocks, and the non-zero blocks are of two types

$$(T1) \quad \pm \begin{pmatrix} x_u & x_{\hat{u}} \\ -x_{\hat{u}} & x_u \end{pmatrix}, \text{ or } (T2) \quad \pm \begin{pmatrix} x_u & -x_{\hat{u}} \\ x_{\hat{u}} & x_u \end{pmatrix}.$$

We construct a complex matrix H from G by substituting to the block (T1) the complex variable $\pm z_u$ and to the block $(T2)$ the complex conjugate variable $\pm z_u^*$. More precisely, the entry of H in position $(w, v) \in W_0 \times V_0$ is

$$H^{w,v} = \begin{cases} (-1)^{f(v+w,v)} z_{v+w}, \text{ if } f(\widehat{v+w}, v) = f(v+w, v), \\ (-1)^{f(v+w,v)} z_{v+w}^*, \text{ otherwise,} \end{cases}$$

if $v + w \in U_0$, and $H^{w,v} = 0$, otherwise.

Theorem 2: The constructed matrix H defines a COD with parameters $[p,\, n,\, k]$.

B. CODs of parameters $\mathbf{LA}_n$

As application of the above procedure, let us reduce the RODs constructed in Section II-D, in order to obtain the optimal CODs of type $\mathbf{LA}_n$. We need to describe here the subsets $U_0, U_1, V_0, V_1, W_0, W_1$ satisfying (3) and (4).

From the expression of f we see that $f(u, \varepsilon^1)$ depends only on the class $|u| \mod 4$. More precisely

$\lvert u\rvert \mod 4$	0	1	2	3
$f(u, \varepsilon^1)$ if $u_1 = 0$	0	0	1	1
$f(u, \varepsilon^1)$ if $u_1 = 1$	0	1	1	0

for an arbitrary $u \in \mathbb{Z}_2^r$.

Case $r = 1, 2 \mod 4$. Let now $u \in U$, so that $|u| = m$ and $r = 2m - 1$ or $2m$. In this case, m is necessarily odd.

- if $m = 1 \mod 4$, then for $u \in U$ we have

  $$f(u, \varepsilon^1) = 0 \Longleftrightarrow u_1 = 0,$$

  in other words,

  $$U_0 = \{u \in U \,|\, u_1 = 0\}, \quad U_1 = \{u \in U \,|\, u_1 = 1\}.$$

  We easily check that

  $$\begin{aligned} V_0 = \{v \in V \,|\, v_1 = 0\}, \quad & V_1 = \{v \in V \,|\, v_1 = 1\}, \\ W_0 = \{w \in W \,|\, w_1 = 0\}, \quad & W_1 = \{w \in W \,|\, w_1 = 1\}. \end{aligned}$$

  satisfies property (4).

- if $m = 3 \mod 4$, then for $u \in U$ we have
$$f(u, \varepsilon^1) = 0 \Longleftrightarrow u_1 = 1,$$
in other words,
$$U_0 = \{u \in U \,|\, u_1 = 1\}, \quad U_1 = \{u \in U \,|\, u_1 = 0\}.$$
We easily check that
$$\begin{aligned} V_0 &= \{v \in V \,|\, v_1 = 0\}, & V_1 &= \{v \in V \,|\, v_1 = 1\}, \\ W_0 &= \{w \in W \,|\, w_1 = 1\} & W_1 &= \{w \in W \,|\, w_1 = 0\}. \end{aligned}$$
again satisfies property (4).

Case $r = 0 \mod 4$. In this case, m is defined by $r = 2m$, so that m is even.

- If $m = 0 \mod 4$, then for $u \in U$ we have
$$f(u, \varepsilon^1) = 0 \Longleftrightarrow u_1 = 1,$$
in other words,
$$U_0 = \{u \in U \,|\, u_1 = 1\}, \quad U_1 = \{u \in U \,|\, u_1 = 0\}.$$
We easily check that
$$\begin{aligned} V_0 &= \{v \in V \,|\, v_1 = 0\}, & V_1 &= \{v \in V \,|\, v_1 = 1\}, \\ W_0 &= \{w \in W \,|\, w_1 = 1\}, & W_1 &= \{w \in W \,|\, w_1 = 0\}. \end{aligned}$$
have the desired property.
- If $m = 2 \mod 4$, then for $u \in U$ we have
$$f(u, \varepsilon^1) = 0 \Longleftrightarrow u_1 = 0,$$
in other words,
$$U_0 = \{u \in U \,|\, u_1 = 0\}, \quad U_1 = \{u \in U \,|\, u_1 = 1\}.$$
We easily check that
$$\begin{aligned} V_0 &= \{v \in V \,|\, v_1 = 0\}, & V_1 &= \{v \in V \,|\, v_1 = 1\}, \\ W_0 &= \{w \in W \,|\, w_1 = 0\} & W_1 &= \{w \in W \,|\, w_1 = 1\}. \end{aligned}$$
have the desired property.

IV. INDUCTION

The second procedure that we call *induction* allows one to transform a $[p, n, k]$-ROD to a $\left[p, n, \frac{k}{2}\right]$-COD. This induction consists in complexification composed with reduction; it can be applied whenever the set U, V and W are stable under an involution $\tilde{u} = u + e$ for an element e satisfying $f(e, e) = 1$.

A. The general construction

STEP 1: We consider the splitting of U as in (3) and define the following subsets of $\mathbb{Z}_2^{r+1} = \mathbb{Z}_2^r \times 0 \sqcup \mathbb{Z}_2^r \times 1$
$$\begin{aligned} U' &= U_0 \times 0 \sqcup U_1 \times 1, \\ V' &= V \times 0 \sqcup V \times 1, \\ W' &= W \times 0 \sqcup W \times 1. \end{aligned}$$

For each $u \in U$, we embed the previous matrix G_u into a twice bigger matrix, $G_{(u,\tau)}$, where $(u, \tau) \in U'$, with columns indexed by W' and rows indexed by V'. The matrix $G_{(u,\tau)}$ is composed by (2×2)-blocks:
$$G_{(u,\tau)} = \begin{array}{c} \begin{array}{c} {\scriptstyle (v,0)(\hat{v},1)} \end{array} \\ \left(\begin{array}{ccc} & \vdots\;\vdots & \\ & \vdots\;\vdots & \\ \begin{array}{c}\cdots\\ \cdots\end{array} & \boxed{\widetilde{G}_u^{w,v}} & \begin{array}{c}\cdots\\ \cdots\end{array} \\ & \vdots\;\vdots & \end{array} \right) \end{array} \begin{array}{c} \\ \\ {\scriptstyle (w,0)} \\ {\scriptstyle (\hat{w},1)} \\ \\ \end{array} ,$$
where the non zero blocks correspond to $(u, \tau) = (v + w, \tau)$ and coincide with those of G_u. These data provide a $[2p, 2n, k]$-ROD.

STEP 2: For each $u \in U_0$, we define
$$G'_u = x_u G_{(u,0)} + x_{\hat{u}} G_{(\hat{u},1)}.$$
These matrices decompose into blocks that are all of type (T1) or (T2). We then apply the reduction procedure to obtain a $\left[p, n, \frac{k}{2}\right]$-ROD.

B. CODs with parameters $\mathbf{TJC}_n$ and $\mathbf{DR}_n$

Consider the RODs of rate 1 constructed in Section II-C.

Following [12], one can apply the following obvious doubling process:
$$G^{(2)} := \begin{pmatrix} G \\ G' \end{pmatrix}$$
where the variables x_u in G are now considered as complex variables, and G' is copy of G associated to the conjugate variables, i.e. is defined by
$$G' = \sum_{u \in U} x_u^* G_u.$$
The matrix $G^{(2)}$ is a COD of rate $\frac{1}{2}$, with parameters
$$\left[2^{\delta(2r)+1},\, 2r,\, 2^{\delta(2r)}\right],$$
that are precisely the parameters of $\mathbf{TJC}_n$, for even n. Removing a column, we are led to CODs with parameters $\mathbf{TJC}_n$, for odd n, except for $n = 1 \mod 8$.

Applying the induction procedure to the RODs of rate 1, leads to CODs with parameters
$$\left[2^{\delta(2r)},\, 2r,\, 2^{\delta(2r)-1}\right],$$
that are precisely the parameters of $\mathbf{DR}_n$, for even n. Again, removing a column, we obtain CODs of type $\mathbf{DR}_n$, for odd n, except for $n = 1 \mod 8$.

In both cases, the obtained CODs have no zero entries.

The missing case $n = 1 \mod 8$ escapes from the technique used in this paper. This is due to the fact that we do not obtain a $[2^r, 2r + 1, 2^r]$-ROD with $n = 0 \mod 4$.

V. Appendices

A. Properties of the functions f and α.

The function f has quite remarkable properties that we briefly discuss here.

It is impossible to reconstruct the function f from the function in one variable α (which is nothing but the restriction of f to the diagonal in $\mathbb{Z}_2^r \times \mathbb{Z}_2^r$). However, α contains the essential characteristics of f, such as its symmetrization.

1) First polarization formula:

$$f(u,v) + f(v,u) = \alpha(u+v) + \alpha(u) + \alpha(v).$$

2) Second polarization formula:

$$\begin{aligned} f(u,v) + f(u,v+w) + f(u+v,w) + f(v,w) = \\ \alpha(u+v+w) \\ +\alpha(u+v) + \alpha(u+w) + \alpha(v+w) \\ +\alpha(u) + \alpha(v) + \alpha(w). \end{aligned}$$

These properties can be checked directly. Note that the expression in the right-hand-side of 1) is called the *coboundary* of α, it has a deep cohomological meaning. The expression in the left-hand-side of 2) is the coboundary of f, its measures the non-associativity of a certain algebra defined by f, see [16]. Finally, the expression in the right-hand-side of 2) is called the *polarization* of the cubic form α. Let us mention that, unlike the theory of quadratic forms, the theory of cubic forms is not well developed in characteristic 2, not much is known.

Let us also give here more elementary properties of f already used in the above constructions:

(a) Linearity of f in 2nd variable:

$$f(u, v+v') = f(u,v) + f(u,v').$$

(b) Pseudo-linearity in 1st variable:

$$f(u+v, v) = f(u,v) + f(v,v).$$

We invite the reader to consult [16] for more information about f and α.

B. Proof of Theorem 1.

We apply the formula for matrices multiplication. The coefficient in position (v,v') in the product $G_u^T G_{u'}$ is

$$(G_u^T G_{u'})^{v,v'} = \begin{cases} (-1)^{f(u,v)+f(u',v')} & \text{if } v+v' = u+u', \\ 0 & \text{otherwise.} \end{cases}$$

This implies that $G_u^T G_{u'} = I_n$, and $G_u^T G_{u'} + G_{u'}^T G_u = 0$ if and only if

$$(-1)^{f(u,v)+f(u',v')} + (-1)^{f(u',v)+f(u,v')} = 0$$

whenever $v+v' = u+u'$. The above condition is equivalent to

$$f(u,v) + f(u',v') + f(u',v) + f(u,v') = 1.$$

Lemma 1: If $u+u' = v+v'$ then

$$f(u,v) + f(u',v') + f(u',v) + f(u,v') = \alpha(u+u').$$

Proof: Rewrite the left-hand-side using $v' = u+u'+v$ and the linearity in the 2nd variable, after cancellation of double terms one obtains

$$f(u',u) + f(u',u') + f(u,u) + f(u,u').$$

This reduces to $\alpha(u+u')$ using the first polarization formula. ■

Theorem 1 follows.

C. Proof of Theorem 2.

First notice that in each column of the matrix H the symbol z_u appears exactly once (“symbol z_u” means one of the following four elements: $\pm z_u, \pm z_u^*$). This implies that the diagonal entries in H^*H are all equal to

$$\sum_{u \in U_0} |z_u|^2.$$

It remains to show that the non-diagonal entries in H^*H are all zero. We show that, in the hermitian product of two distinct columns of H, the terms pairwise cancel.

Consider the four entries of H, in position (w,v), (w',v), (w',v) and (w',v').

$$H = \begin{array}{c} \begin{array}{ccccc} & v & & v' & \end{array} \\ \left(\begin{array}{ccccc} & \vdots & & \vdots & \\ \cdots & z_1 & \cdots & z_2 & \cdots \\ & \vdots & & \vdots & \\ \cdots & z_3 & \cdots & z_4 & \cdots \\ & \vdots & & \vdots & \end{array} \right) \end{array} \begin{array}{c} \\ \\ w \\ \\ w' \\ \\ \end{array}$$

Case I: there exist u, u' in U_0 such that

$$u = v + w = v' + w', \quad u' = v + w' = v' + w.$$

In this case, the four entries are non zero and one has

$$z_1, z_4 \in \{\pm z_u, \ \pm z_u^*\}, \quad z_2, z_3 \in \{\pm z_{u'}, \ \pm z_{u'}^*\}.$$

The corresponding blocks in the matrix G

$$G = \left(\begin{array}{ccccc} & \vdots & & \vdots & \\ \cdots & A_1 & \cdots & A_2 & \cdots \\ & \vdots & & \vdots & \\ \cdots & A_3 & \cdots & A_4 & \cdots \\ & \vdots & & \vdots & \end{array} \right)$$

come from $x_u G_u + x_{\hat{u}} G_{\hat{u}} + x_{u'} G_{u'} + x_{\hat{u}'} G_{\hat{u}'}$ and therefore satisfy

$$A_1^T A_2 + A_3^T A_4 = 0.$$

This translates to

$$z_1^* z_2 + z_3^* z_4 = 0.$$

Case II: there do not exist u, u' in U_0 such that

$$u = v + w = v' + w', \quad u' = v + w' = v' + w.$$

In this case at least one of the following situations holds

$$z_1 = z_4 = 0 \quad \text{or} \quad z_2 = z_3 = 0,$$

and, again, $z_1^* z_2 + z_3^* z_4 = 0$.

We have proved that the columns of H are pairwise orthogonal (with respect to the hermitian product). And we conclude finally that

$$H^* H = \left(\Sigma_{u \in U_0} |z_u|^2\right) I_n$$

where $n = \# V_0$.

D. Orthogonal designs and Hurwitz problem of sums of squares

It is well-known that the existence of $[p, n, k]$-ROD is related to the Hurwitz problem on composition of quadratic forms, [14],[17] (see also [20] for a survey).

Definition 5: A Hurwitz sum of squares identity (SSI) of size $[p, n, k]$ is an identity

$$\left(a_1^2 + \cdots + a_k^2\right)\left(b_1^2 + \cdots + b_n^2\right) = c_1^2 + \cdots + c_p^2, \qquad (5)$$

where c_i are bilinear expressions in a_i and b_i with integral coefficients (the elements a_i, b_i, c_i's are considered here as real variables). Such an identity will be referred as a $[p, n, k]$-identity.

It is known that if such an identity holds then the integral coefficients in the expressions of c_i's can be chosen among $\{0, 1, -1\}$. Hurwitz proved the following fundamental theorem. *There exists a $[p, n, k]$-ROD if and only if there exists a $[p, n, k]$-SSI.*

Let us recall here how the equivalence can be established. Since c's are linear in a's and b's, one has

$$c = \left(\sum_{1 \leq i \leq k} a_i A_i\right) b, \qquad (6)$$

where b is a column-vector with components b_i and c is a column-vector with components c_i, and where A_i are $p \times n$ matrices (with entries $0, 1, -1$) One then easily checks that the identity (6) holds if and only if

$$A_i^T\, A_i = I_n, \quad A_i^T A_j + A_j^T A_i = 0, \quad \forall\, i \neq j. \qquad (7)$$

Then, the matrix $A = \left(\sum_{1 \leq i \leq k} a_i A_i\right)$ is a $[p, n, k]$-ROD in the variables a_i's.

A classical result of Hurwitz [13] states that $[n, n, n]$-SSI exist if and only if $n = 1, 2, 4, 8$. This statement relies on classification of normed division algebras, see [19] for a survey on relations between division algebras and wireless communications. The case of $[n, n, k]$-SSI was solved independently by Hurwitz [14] and Radon [17], this is the origin of the famous Hurwitz-Radon function.

Let us mention that our previous results [16] and [15] were formulated in terms of partial solutions to the Hurwitz problem.

References

[1] S. Spence Adams, N. Karst and J. Pollak, "The Minimum Decoding Delay of Maximal Rate Complex Orthogonal Space-Time Block Codes," *IEEE Trans. Inform. Theory,* vol. 53, No. 8, pp. 2677-2684, Aug. 2007.

[2] S. Spence Adams, N. Karst and M. Kishore Murugan, "The Final Case of the Decoding Delay Problem for Maximum Rate Complex Orthogonal Designs," *IEEE Trans. Inform. Theory,* vol. 56, No. 1, pp. 103-112, Jan. 2010.

[3] S.M. Alamouti, "A Simple Transmit Diversity Technique For Wireless Communications", *IEEE J. Select. Areas Commun.* Vol 16, pp 1451–1458, Oct. 1998.

[4] S. Das and B. Sundar Rajan, "A novel construction of complex orthogonal designs with maximal rate and low-PAPR," *Information Theory, 2009. ISIT 2009. IEEE International Symposium,* pp. 89–93, 2009.

[5] S. Das and B. Sundar Rajan, "Low-delay, High-rate Non-square Complex Orthogonal Designs", arXiv:1112.1593.

[6] A. V. Geramita, J..M. Geramita, J. Seberry, "Orthogonal designs," *Linear and Multilinear Algebra* 3 (1975/76), no. 4, 281–306.

[7] A. V. Geramita and N. J. Pullman, "A theorem of Hurwitz and Radon and Orthogonal projective modules," *Proc. Amer. Math. Soc.,* vol. 42, No. 1, pp. 51-56, Jan. 1974.

[8] A. V. Geramita, J. Seberry, "Orthogonal designs. Quadratic forms and Hadamard matrices." Lecture Notes in Pure and Applied Mathematics, 45. Marcel Dekker, Inc., New York, 1979.

[9] A. V. Geramita, J. Geramita, "Complex orthogonal designs." *J. Combin. Theory Ser. A* 25 (1978), no. 3, 211–225.

[10] X. B. Liang "Orthogonal Designs with Maximal Rates," *IEEE Trans. Inform. Theory,* Vol. 49, no. 10, pp. 2468–2503, Oct. 2003.

[11] K. Lu, S. Fu and X.-G. Xia, "Closed-Form Designs of Complex Orthogonal Space-Time Block Codes of Rates $\frac{k+1}{2k}$ for $2k-1$ or $2k$ Transmit Antennas," *IEEE Trans. Inform. Theory,* vol. 51, No. 5, pp. 4340–4347, Dec. 2005.

[12] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Space-time block codes from orthogonal designs," *IEEE Trans. Inform. Theory,* vol. 45, no. 5, pp. 1456–1467, July 1999.

[13] A. Hurwitz, "Uber die Komposition der quadratischen Formen von beliebig vielen Variablen", Nahr. Ges. Wiss. Göttingen (1898), 309–316.

[14] A. Hurwitz, "Uber die Komposition der quadratischen Formen", *Math. Ann.* 88 (1922), 1–25.

[15] A. Lenzhen, S. Morier-Genoud, V. Ovsienko, "New solutions of the Hurwitz problem on square identities", *J. of Pure App. Alg.*, 215 (2011), 2903–2911.

[16] S. Morier-Genoud, V. Ovsienko, "A series of algebras generalizing the octonions and Hurwitz-Radon identity", *Comm. Math. Phys.* 306 (2011), no. 1, 83–118.

[17] J. Radon, "Lineare scharen orthogonale Matrizen", *Abh. Math. Sem. Univ.* Hamburg **1** (1922) 1–14.

[18] A.R. Rajwade, Squares. London Mathematical Society Lecture Note Series, 171. Cambridge.

[19] B.A. Sethuraman, "Division algebras and wireless communication", Notices Amer. Math. Soc. 57 (2010), no. 11, 1432–1439.

[20] D. B. Shapiro, Compositions of Quadratic forms, Berlin, Germany: Walter de Gruyter, 2000.