Orthogonal designs and a cubic binary function
Sophie Morier-Genoud, Valentin Ovsienko

To cite this version:
Sophie Morier-Genoud, Valentin Ovsienko. Orthogonal designs and a cubic binary function. IEEE Transactions on Information Theory, Institute of Electrical and Electronics Engineers, 2013, 59 (3), pp.1583–1589. 10.1109/TIT.2012.2229335. hal-00864648

HAL Id: hal-00864648
https://hal.archives-ouvertes.fr/hal-00864648
Submitted on 23 Sep 2013

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
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 designs maximizing the rate and minimizing the decoding delay.

Case 247, 4 pl. Jussieu, 75005 Paris, France; sophiemg@math.jussieu.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
\[
G^T G = (x_1^2 + \cdots + x_k^2) I_n,
\]

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
\[
H^* H = (|z_1|^2 + \cdots + |z_k|^2) I_n,
\]

where \(H^*\) is the complex conjugate transpose of \(H\).

Definition 3: Given a \([p,n,k]\)-ROD or COD, 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
\[
\delta(n) = \begin{cases} 
\frac{n}{2} & \text{if } n = 2, 4, 6 \pmod{8}, \\
\frac{n-1}{2} & \text{if } n = 1, 7 \pmod{8}, \\
\frac{n+1}{2} & \text{if } n = 3, 5 \pmod{8}, \\
\frac{n}{2} - 1 & \text{if } n = 0 \pmod{8}. 
\end{cases}
\]

This is a way to formulate the classical theorem of 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 \(TJC_n\) 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 \(n = 0, 1, 3 \pmod{4}\) and
\[
p \geq 2\binom{2m}{m-1},
\]
for $n = 2 \mod 4$. We will denote by $\text{LA}_n$ 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 $\text{LA}_n$. 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 $\text{DR}_n$ 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 $\text{TJC}_n$.

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 $\text{LA}_{n}$ has rate $\frac{7}{12}$ and decoding delay 792, whereas $\text{DR}_n$ has rate $\frac{1}{2}$ and decoding delay 64, see [5] for a comparative table.

\section{General construction of RODs}

\subsection{Combinatorics over $\mathbb{Z}_2$}

We denote by $\mathbb{Z}_2^n$ the set of $r$-vectors $u = (u_1, \ldots, u_r)$, where $u_i = 0$ or 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 component-wise 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 $r$:

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

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

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

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

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 $\alpha$ is used as a “statistic” to select good elements of $\mathbb{Z}_2^n$. Properties of $f$ and $\alpha$ are presented in Appendix.

\subsection{General construction of RODs}

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

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

$$G_u = \begin{pmatrix} v \\ \vdots \\ \cdots \\ G_{u, w}^w \vdots \\ \cdots \\ \vdots \\
\end{pmatrix}$$

where the entry in position $(w, v)$ is

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

\footnote{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 $V = W = \mathbb{Z}_2$, 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
   
   $\alpha(u + u') = \alpha(v + v') = 1$. \hspace{1cm} (2)

**Theorem 1:** If $U, V, W$ is an admissible triple, then one has:

(i) $G_u^T G_u = I_r$, for all $u \in U$.
(ii) $G_u^T G_w + G_w^T G_u = 0$, 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 $\alpha$ 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 $[2^h(n), n, 2^h(n)]$, (provided $n \neq 1 \mod 8$).

**Case $r = 0, 1, 2 \mod 4.$** One chooses the following subsets

$V = \{\varepsilon, \hat{\varepsilon}, \varepsilon^j, \hat{\varepsilon}^j, 1 \leq j \leq r\}$,

$U = W = \mathbb{Z}_2$,

where $^\dagger$ is the duality (1). Then $G$ is a $[2^r, 2r, 2^r]$-ROD. \hspace{1cm} \footnote{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

$V = \{\varepsilon, \hat{\varepsilon}, \varepsilon^j, \hat{\varepsilon}^j, 1 \leq j \leq r\}$,

$U = W = \mathbb{Z}_2^r$,

the $G$ is a $[2^r, 2r + 2, 2^r]$-ROD.

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

All the RODs below have maximal rate $\frac{1}{2} + \frac{1}{2^m}$, 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:

$U = \{u, v : |u| = m\}$,

$V = \{\varepsilon^j, \hat{\varepsilon}^j, 1 \leq j \leq r\}$.

It follows that the space $W = U + V$ is:

$W = \{u : |u| = m - 1, m + 1\} \cup \{u : u_1 = 1, |u| = m + 2\} \cup \{u : u_1 = 0, |u| = m - 2\}$.

The matrix $G$ is a ROD with parameters

$[2\binom{r+1}{m-1}, 2r, 2\binom{r}{m}]$, \hspace{1cm} $[4\binom{r}{m-1}, 2r, 2\binom{r}{m}]$,

for odd $r$ and even $r$, respectively.

**Case $r = 0 \mod 4.$** Consider $r = 2m$ (where $m$ is even) and choose the following subsets

$U = \{u : u_1 = 1, |u| = m\} \cup \{u : u_1 = 0, |u| = m - 1\}$,

$V = \{\varepsilon^j, \hat{\varepsilon}^j, 2 \leq j \leq n\}$,

$W = \{u : u_1 = 1, |u| = m - 1, m + 1\} \cup \{u : u_1 = 0, |u| = m - 2\}$,

then $G$ is a $[2\binom{r}{m-1}, 2r, 2\binom{r-1}{m-1}]$-ROD.

**Case $r = 3 \mod 4.$** Consider $r' := r + 1$ and apply the previous case with $r' = 0 \mod 4$ to obtain a $[2\binom{r+1}{m-1}, 2r + 2, 2\binom{r}{m}]$-ROD, where $r = 2m - 1$. Removing two columns, we obtain a $[2\binom{r+1}{m-1}, 2r, 2\binom{r}{m}]$-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
\[ \tilde{\wedge} : \mathbb{Z}_2^p \to \mathbb{Z}_2^p \]
defined by $\hat{u} = u + e$, where the element $e \in \mathbb{Z}_2^p$ satisfies $f(e, e) = 1$, and to choose sets $U, V$ and $W$ stable under the duality:
\[ \hat{U} = U, \quad \hat{V} = V, \quad \hat{W} = W, \]
In practice, we use the hat duality (1), i.e., $e = e^1$.

Given a ROD of type $[2p, 2n, 2k]$ defined by sets $U, V$ and $W$ in $\mathbb{Z}_2^p$, 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 $U, V, W$ and $U, V$. We now need to find subsets $U_0, V_0, W_0$ and $W_1$ satisfying the following conditions
\[ V = V_0 \cup V_1, \quad V_1 = \tilde{V}_0, \]
\[ W = W_0 \cup W_1, \quad W_1 = \tilde{W}_0; \]
\[ W_0 = U_0 + V_0 = U_1 + V_1; \]
\[ W_1 = U_0 + V_1 = U_1 + V_0, \]
where $\cup$ denotes the disjoint union.

These splitting induce a natural decomposition of the matrices $G_u$ into $(2 \times 2)$-blocks whose columns are labelled by $(v, \hat{v}) \in V_0 \times V_1$ and the rows by $(w, \hat{w}) \in W_0 \times W_1$:
\[
G_u = \begin{pmatrix}
  v & \hat{v} \\
  \vdots & \vdots \\
  \vdots & \vdots \\
  \vdots & \vdots \\
 w & \hat{w}
\end{pmatrix}
\]
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
\[
\tilde{G}^{w,v}_u = \begin{pmatrix}
  (−1)^{f(u,v)} & 0 \\
  0 & (−1)^{f(u,v)}
\end{pmatrix}
\]
and non-zero blocks are located at the same place in $G_u$ and $\tilde{G}_u$. Moreover, since $f$ is linear in the 2nd variable,
\[
f(u, \hat{v}) = f(u, v) + f(u, e) = f(u, v),
\]
\[
f(\hat{u}, \hat{v}) = f(\hat{u}, v) + f(\hat{u}, e) = f(\hat{u}, v) + 1,
\]
so that the entries in the blocks of $\tilde{G}_u$ 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 $(2 \times 2)$-blocks, and the non-zero blocks are of two types
\[ (T1) \pm \begin{pmatrix}
  x_u & x_{\hat{v}} \\
  -x_{\hat{u}} & x_u
\end{pmatrix}, \text{ or } (T2) \pm \begin{pmatrix}
  x_u & -x_{\hat{u}} \\
 -x_{\hat{v}} & x_u
\end{pmatrix}. \]
We construct a complex matrix $H$ from $G$ by substituting to the block (T1) the complex variable $z_u$ and to the block (T2) the complex conjugate variable $\pm z^*_u$. More precisely, the entry of $H$ in position $(w, v)$ is $0$ 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 $\mathbb{L}A_n$

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 $\mathbb{L}A_n$. 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 $f(u, e^1)$ depends only on the class $|u| \mod 4$. More precisely
\[
\begin{array}{c|cccc}
|u| \mod 4 & 0 & 1 & 2 & 3 \\
\hline
f(u, e^1) & 0 & 0 & 1 & 1 \\
\end{array}
\]
for an arbitrary $u \in \mathbb{Z}_2^p$.

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
\[
f(u, e^1) = 0 \iff u_1 = 0,
\]
in other words,
\[
U_0 = \{ u \in U \mid u_1 = 0 \}, \quad U_1 = \{ u \in U \mid u_1 = 1 \}.
\]

We easily check that
\[
V_0 = \{ v \in V \mid v_1 = 0 \}, \quad V_1 = \{ v \in V \mid v_1 = 1 \}, \quad W_0 = \{ w \in W \mid w_1 = 0 \}, \quad W_1 = \{ w \in W \mid w_1 = 1 \}.
\]
satisfies property (4).
- if \( m = 3 \mod 4 \), then for \( u \in U \) we have
  \[ f(u, e^1) = 0 \iff u_1 = 1, \]
in other words,
  \[ U_0 = \{ u \in U \mid u_1 = 1 \}, \quad U_1 = \{ u \in U \mid u_1 = 0 \}. \]

We easily check that
  \[ V_0 = \{ v \in V \mid v_1 = 0 \}, \quad V_1 = \{ v \in V \mid v_1 = 1 \}, \]
  \[ W_0 = \{ w \in W \mid w_1 = 1 \}, \quad W_1 = \{ w \in W \mid w_1 = 0 \}. \]

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
  \[ f(u, e^1) = 0 \iff u_1 = 1, \]
in other words,
  \[ U_0 = \{ u \in U \mid u_1 = 1 \}, \quad U_1 = \{ u \in U \mid u_1 = 0 \}. \]

We easily check that
  \[ V_0 = \{ v \in V \mid v_1 = 0 \}, \quad V_1 = \{ v \in V \mid v_1 = 1 \}, \]
  \[ W_0 = \{ w \in W \mid w_1 = 1 \}, \quad W_1 = \{ w \in W \mid w_1 = 0 \}. \]

have the desired property.
- If \( m = 2 \mod 4 \), then for \( u \in U \) we have
  \[ f(u, e^1) = 0 \iff u_1 = 0, \]
in other words,
  \[ U_0 = \{ u \in U \mid u_1 = 1 \}, \quad U_1 = \{ u \in U \mid u_1 = 1 \}. \]

We easily check that
  \[ V_0 = \{ v \in V \mid v_1 = 0 \}, \quad V_1 = \{ v \in V \mid v_1 = 1 \}, \]
  \[ W_0 = \{ w \in W \mid w_1 = 0 \}, \quad W_1 = \{ w \in W \mid w_1 = 1 \}. \]

have the desired property.

**IV. Induction**

The second procedure that we call *induction* allows one to transform a \([p, n, k]\)-COD to a \([p, n, \frac{k}{2}]\)-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 \( \bar{u} = u + e \) 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 \( \mathbb{Z}_2^{r+1} = \mathbb{Z}_2^r \times 0 \sqcup \mathbb{Z}_2^r \times 1 \)
  \[ U' = U_0 \times 0 \sqcup U_1 \times 1, \]
  \[ V' = V \times 0 \sqcup V \times 1, \]
  \[ W' = W \times 0 \sqcup W \times 1. \]

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 \((2 \times 2)\)-blocks:

\[
G_{(u,\tau)} = \begin{pmatrix}
(v,0)(\bar{v},1) \\
\vdots & \ddots & \ddots \\
\vdots & \ddots & G_{u,v} & \ddots \\
\vdots & \ddots & \ddots & \ddots & \ddots \\
(w,0) & \ddots & \ddots & \ddots & \ddots & (w,1)
\end{pmatrix},
\]

where the non zero blocks correspond to \((u, \tau) = (v + w, \tau)\) and coincide with those of \( G_u \). These data provide a \([2p, 2n, k]\)-COD.

**STEP 2**: For each \( u \in U_0 \), we define
\[
G'_u = x_u G_{(u,0)} + x_{\bar{u}} G_{(\bar{u},1)}.
\]

These matrices decompose into blocks that are all of type (T1) or (T2). We then apply the reduction procedure to obtain a \([p, n, \frac{k}{2}]\)-COD.

**B. CODs with parameters \( \text{TJC}_n \) and \( \text{DR}_n \)**

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 \( \text{TJC}_n \), for even \( n \). Removing a column, we are led to CODs with parameters \( \text{TJC}_n \), 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 \( \text{DR}_n \), for even \( n \). Again, removing a column, we obtain CODs of type \( \text{DR}_n \), 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 \([2^r, 2r + 1, 2^r]\)-COD with \( n = 0 \mod 4 \).
V. APPENDICES

A. Properties of the functions \( f \) and \( \alpha \).

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 \( \alpha \) (which is nothing but the restriction of \( f \) to the diagonal in \( \mathbb{Z}_2^2 \times \mathbb{Z}_2^2 \)). However, \( \alpha \) 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:
\[
f(u,v) + f(u,v+w) + f(u+v,w) + f(v,w) = \\
\alpha(u + v + w) + \alpha(u + v) + \alpha(u + w) + \alpha(v + w) + \alpha(u) + \alpha(v) + \alpha(w).
\]

These properties can be checked directly. Note that the expression in the right-hand-side of 1) is called the coboundary of \( \alpha \), 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 \( \alpha \). 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 \( \alpha \).

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 \( H^T H \) are all equal to
\[
\sum_{u \in U_0} |z_u|^2.
\]

It remains to show that the non-diagonal entries in \( H^T H \) 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 \((w',v')\).

**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 \( G \)
\[
G = \begin{pmatrix}
\cdots & A_1 & \cdots & A_2 & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
\cdots & A_3 & \cdots & A_4 & \cdots \\
\end{pmatrix}
\]

come from \( x_u G_u + x_{u'} G_{u'} + x_{u'}^* G_u + x_u^* G_{u'} \) 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, $z_1^2 z_2 + z_3^2 z_4 = 0$.

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

$$H^* H = \left( \sum_{a \in V_0} |z_a|^2 \right) I_n$$

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

$$(a_1^2 + \cdots + a_k^2) (b_1^2 + \cdots + b_n^2) = c_1^2 + \cdots + c_p^2,$$  \hspace{1cm} (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

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

$$A_i^T A_i = I_n, \quad A_i^T A_j + A_j^T A_i = 0, \quad \forall i \neq j.$$  \hspace{1cm} (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**


