Operations Research
Report 2011-02

Multiplically independent word systems

Miklós Ujvári

September 2011

Eötvös Loránd University of Sciences
Department of Operations Research

ISSN 1215 - 5918

Multiplically independent word systems

Miklós Ujvári

Abstract

Tressler's Theorem states that the long-standing Hadamard conjecture (concerning the existence of n by n orthogonal matrices with elements of the same absolute value, for $n = 4k$, $k = 1, 2, \ldots$) will be settled if we find $n - 2$ pairwise orthogonal words in a hyperplane of words. In this paper we will prove the counterpart of Tressler's Theorem: the existence of $n - 2$ multiplically independent words in a hyperplane of words.

Mathematics Subject Classifications (2000). 90C22, 90C27, 05B20.

1 Introduction

We start the paper with describing our motivation for studying the Hadamard conjecture.

We call a matrix $H \in \{\pm 1\}^{m \times n}$ an *Hadamard matrix* if its column vectors are pairwise orthogonal, that is $H^T H = mI$ (with ^{T} denoting transpose and I the identity matrix). The long-standing *Hadamard conjecture* states that there exists an Hadamard matrix $H \in \{\pm 1\}^{n \times n}$ if $n \equiv 0 \pmod 4$. Presently, the Hadamard conjecture is verified for all $n < 668$ (see [2]), and for some infinite classes of n (see [6], [4]). For a historical overview and applications we refer to [7], [1].

Our motivation concerning Hadamard matrices comes from graph theory, more closely representations of graphs with orthovectors (see [8]). We call *orthovector* a block matrix $(A_1^T, \ldots, A_d^T)^T \in (\mathcal{R}^{m \times m})^d$ where each block A_i is of the form $\alpha_i O_i$, a constant $\alpha_i \in \mathcal{R}$ multiplied by an orthogonal matrix $O_i \in \mathcal{R}^{m \times m}$, $O_i^T = O_i^{-1}$. Orthovector representations of graphs are particularly interesting when for the representing orthovectors (A_i) the orthogonal

matrices O_i are elements of a fixed *Hadamard matrix system*,

$$OD_{h_1}O^T, \ldots, OD_{h_n}O^T \in \mathcal{R}^{m\times m}$$

where $O \in \mathcal{R}^{m\times m}$, $O^T = O^{-1}$ is an orthogonal matrix and the column vectors $h_1, \ldots, h_n \in \{\pm 1\}^m$ form an Hadamard matrix $H \in \{\pm 1\}^{m\times n}$. (Here D_v denotes the diagonal matrix with vector v on its diagonal.)

In [9] we reformulated the Hadamard conjecture using Hurwitz-Radon word systems. Let us recall the necessary definitions and the main result of [9].

We are given an alphabet $\mathcal{A} = \{a, b, c, d\}$ which is a Klein group with multiplication table:

$\cdot$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

Words of the same length s and made up of the letters in $\mathcal{A}$ are multiplied letterwise: if $W_1, W_2 \in \mathcal{A}^s$ then their *product* is an s-letter word, denoted by $W_1 \cdot W_2$, whose i-th letter is the product of the i-th letter of W_1 and the i-th letter of W_2 $(1 \le i \le s)$.

A word system $W_1, \ldots, W_n \in \mathcal{A}^s$ is called a *Hurwitz-Radon word system* if the product $W_i \cdot W_j$ contains an odd number of the letter bs, for each pair of words W_i, W_j $(i \ne j)$ from the system. An example is the word system $\mathcal{R}_n$, defined in Section 2, which is a Hurwitz-Radon word system made up of n words in $\mathcal{A}^{\sigma(n)}$. Here $\sigma(n)$ denotes the number of integers s in the range $0 < s < n$ such that $s \equiv 0, 1, 2,$ or $4 \pmod 8$.

A word system $W_1, \ldots, W_n \in \mathcal{A}^s$ can be considered as a matrix from $\mathcal{A}^{n\times s}$ whose rows are formed by the words $W_1, \ldots, W_n$. In this case we speak about a *row system of words*, and we do not differentiate in the notation between the word system and the corresponding matrix, they are both denoted by $\mathcal{W}$. A *column system of words* can be defined similarly. We denote by $[\mathcal{W}']$ that the word system $\mathcal{W}'$ is considered as a column system. The corresponding matrix of letters is denoted similarly.

Given two words $W \in \mathcal{A}^{1\times s}$ and $[W'] \in \mathcal{A}^{s\times 1}$, their *symmetricity product* $W[W']$ is defined as the total number of the letter bs in the word $W \cdot W'$ taken modulo 2. For two word systems $\mathcal{W} = (W_1, \ldots, W_n) \in \mathcal{A}^{n\times s}$ and $\mathcal{W}' = (W'_1, \ldots, W'_m) \in \mathcal{A}^{m\times s}$, their *symmetricity product* is the matrix $\mathcal{W}[\mathcal{W}'] \in \{0,1\}^{n\times m}$ whose (i,j)-th element is $W_i[W'_j]$ for all $1 \le i \le n$, $1 \le j \le m$.

With this notation $\mathcal{W}$ is a Hurwitz-Radon word system if and only if $\mathcal{W}[\mathcal{W}] = J - I$, where J denotes the matrix with all elements equal to one.

The main result of [9] is described in the following theorem. The word set $\hat{\mathcal{H}}_n \subseteq \mathcal{A}^{\sigma(n)}$ is defined in Section 4.

THEOREM 1.1. *Let $n \equiv 0 \pmod 4$. Then, there exists an Hadamard matrix $H \in \{\pm 1\}^{n\times n}$ if and only if there exists a word system $\mathcal{H} \subseteq \mathcal{A}^{\sigma(n)}$ for which the following statements hold: a) the number of different words in $\mathcal{H}$ is $n-1$; b) $\mathcal{H} \subseteq \hat{\mathcal{H}}_n$; c) for any two different words H_1, H_2 from $\mathcal{H}$, their product $H_1 \cdot H_2$ is in $\hat{\mathcal{H}}_n$.*

Theorem 1.1 can be sharpened using Tressler's Theorem in [7].

THEOREM 1.2. (Tressler) *Let $n \equiv 0 \pmod 4$. Then, there exists an Hadamard matrix $H \in \{\pm 1\}^{n\times n}$ if and only if there exists an Hadamard matrix $H' \in \{\pm 1\}^{n\times(n-1)}$.*

As an immediate consequence of Theorems 1.1 and 1.2 we obtain

THEOREM 1.3. *Let $n \equiv 0 \pmod 4$. Then, there exists an Hadamard matrix $H \in \{\pm 1\}^{n\times n}$ if and only if there exists a word system $\mathcal{H} \subseteq \mathcal{A}^{\sigma(n)}$ for which the following statements hold: a) the number of different words in $\mathcal{H}$ is $n-2$; b) $\mathcal{H} \subseteq \hat{\mathcal{H}}_n$; c) for any two different words H_1, H_2 from $\mathcal{H}$, their product $H_1 \cdot H_2$ is in $\hat{\mathcal{H}}_n$.* □

We will call a word system $W_1, \ldots, W_m \in \mathcal{A}^{\sigma(n)}$ *multiplically independent* if

$$\left.\begin{array}{r} W_1^{\varepsilon_1} \cdot \ldots \cdot W_m^{\varepsilon_m} = a \ldots a \\ \varepsilon_1, \ldots, \varepsilon_m \in \{0,1\} \end{array}\right\} \text{ implies } \varepsilon_1 = \ldots = \varepsilon_m = 0,$$

where $W^0 := a \ldots a$ and $W^1 := W$ for any $W \in \mathcal{A}^{\sigma(n)}$. Equivalently, the word system $W_1, \ldots, W_m \in \mathcal{A}^{\sigma(n)}$ is multiplically independent if and only if its *generated word set*,

$$\langle W_1, \ldots, W_m \rangle := \{W_1^{\varepsilon_1} \cdot \ldots \cdot W_m^{\varepsilon_m} : \varepsilon_1, \ldots, \varepsilon_m \in \{0,1\}\}$$

is of cardinality 2^m.

The main result of this paper (see also Theorem 4.3) is described in

THEOREM 1.4. *Let $n \equiv 0 \pmod 4$. Then, there exists a multiplically independent word system $W_1, \ldots, W_{n-2}$ in the word set $\hat{\mathcal{H}}_n \cap \langle \mathcal{R}_n \rangle$.*

The structure of the paper is as follows: In Section 2 we will prove some basic results concerning the word system $\mathcal{R}_n$ and its generated word set $\langle \mathcal{R}_n \rangle$. In Section 3 some refinements and simplified proofs of results of [9] concerning image vectors $\mathcal{R}_n[\mathcal{A}^{\sigma(n)}]$ are described. Finally, in Section 4 we will study properties of the word set $\hat{\mathcal{H}}_n \cap \langle \mathcal{R}_n \rangle$, and derive Theorems 1.4, 4.3.

2 The word sets $\mathcal{R}_n$ and $\langle \mathcal{R}_n \rangle$

In this section some elementary properties of the word system $\mathcal{R}_n$ and the generated word set $\langle \mathcal{R}_n \rangle$ are described.

Let us recall the inductive definition of the word system $\mathcal{R}_n$ (see [8], [9]). For $n = 2, 4, 8, 9$, $\mathcal{R}_n$ is defined as

$$\begin{array}{ll} n = 2,\ \sigma(n) = 1: & a, b \\ n = 4,\ \sigma(n) = 2: & aa, cb, ba, db \\ n = 8,\ \sigma(n) = 3: & aaa, ccb, cba, cdb, baa, dab, dbc, dbd \\ n = 9,\ \sigma(n) = 4: & aaaa, accb, acba, acdb, abaa \\ & adab, adbc, cdbd, ddbd. \end{array}$$

Now, suppose that for some n the word system $\mathcal{R}_n$ is already constructed. Denote by $T_1, \ldots, T_n$ the words in $\mathcal{R}_n$, and also by $S_1, \ldots, S_9$ the words in $\mathcal{R}_9$. (We will use these notations throughout the paper.) Then, $\mathcal{R}_{n+8}$ is defined as the word system made up of the words

$$S_1 \& T_1, \ldots, S_9 \& T_1,\ bdbd \& T_2, \ldots, bdbd \& T_n,$$

where & denotes concatenation of words. This way we defined the word system $\mathcal{R}_n \subseteq \mathcal{A}^{\sigma(n)}$ for all $n \equiv 0, 1, 2, 4 \pmod 8$.

Note that to prove a statement concerning the word systems $\mathcal{R}_n$ for all $n \equiv 0, 1, 2, 4 \pmod 8$, it is enough to prove it for $n = 2, 4, 8, 9$, then, assuming that the statement holds for n, to prove is for $n + 8$. In what follows, we will refer to this induction step shortly as the $n \to n + 8$ step.

PROPOSITION 2.1. *Let $n = 4, 8, \ldots$. Then, $\prod \mathcal{R}_n = a \ldots a$.*

Proof. We use induction based on the definition of $\mathcal{R}_n$. The cases when $n = 4, 8$ can be verified directly. In the $n \to n + 8$ step, assuming $\prod \mathcal{R}_n = a \ldots a$, we have to prove the equation

$$\prod_{i=1}^{9} (S_i \& T_1) \cdot \prod_{j=2}^{n} (bdbd \& T_j) = a \ldots a,$$

which follows by the equation $\prod \mathcal{R}_9 = bdbd$. □

Another useful property of $\mathcal{R}_n$ is that any subsystem with $n - 2$ nontrivial elements is multiplically independent.

PROPOSITION 2.2. *Let $n = 4, 8, \ldots$. Then, leaving out from $\mathcal{R}_n$ its first word $a \ldots a$ and another word, too, we obtain a multiplically independent word system.*

Proof. We use induction based on the definition of $\mathcal{R}_n$. The cases when $n = 4, 8$ can be verified directly. For the $n \to n + 8$ step, let us suppose indirectly, that

$$\prod_{i\in K}(S_i\&T_1)\cdot\prod_{j\in L}(bdbd\&T_j) = a\dots a,$$

where $K \subseteq \{2,\dots,9\}$, $L \subseteq \{2,\dots,n\}$, and the former or the latter inclusion is strict. We distinguish these two cases.

Case 1: $K \subset \{2,\dots,9\}$. It can be easily verified, that $\prod_{i\in K} S_i \neq aaaa, bdbd$.

Case 2: $L \subset \{2,\dots,n\}$. By the inductional assumption $\prod_{j\in L} T_j \neq a\dots a$.

In both cases we reached contradiction with the indirect assumption, the proof is finished. □

As an immediate consequence of Proposition 2.2 we obtain

THEOREM 2.1. *Let $n = 4, 12, \dots$. Then, $\langle\mathcal{R}_n\rangle = \mathcal{A}^{\sigma(n)-2}\&\mathcal{R}_4$. (In other words, the word system $\mathcal{R}_n$ generates the set of words ending in the letter pairs aa, cb, ba, db.)*

Proof. As the inclusion $\langle\mathcal{R}_n\rangle \subseteq \mathcal{A}^{\sigma(n)-2}\&\mathcal{R}_4$ is obvious, it is enough to notice that by Proposition 2.2 the cardinalities of these two word sets are equal. □

The following theorem can be proved analogously as Theorem 2.1.

THEOREM 2.2. *Let $n = 8, 16, \dots$. Then, $\langle\mathcal{R}_n\rangle = \mathcal{A}^{\sigma(n)}$.* □

Finally, we will derive another description of the generated word set $\langle\mathcal{R}_n\rangle$. To this end, for an arbitrary word $W \in \mathcal{A}^{\sigma(n)}$ let us denote

$$W^{\mathcal{R}_n} := \prod_{i=1}^{n} T_i^{\mathcal{R}_n[W]_i} \in \mathcal{A}^{\sigma(n)}.$$

(Note that $\mathcal{R}_n[W]_i = T_i[W]$ by the definition of the word T_i.) We will show that the mapping $.^{\mathcal{R}_n}$ commutes with multiplication on $\mathcal{A}^{\sigma(n)}$. (Here $v_1 +_2 v_2$ denotes addition of vectors $v_1, v_2 \in \{0,1\}^n$ modulo 2, and $\overline{v}$ the negation of the vector $v \in \{0,1\}^n$.)

PROPOSITION 2.3. *Let $n = 4, 8, \dots$. Then,*

$$W_1^{\mathcal{R}_n}\cdot W_2^{\mathcal{R}_n} = (W_1\cdot W_2)^{\mathcal{R}_n}$$

for any words $W_1, W_2 \in \mathcal{A}^{\sigma(n)}$.

Proof. By Proposition 2.1 we have

$$\begin{aligned} W_1^{\mathcal{R}_n} \cdot W_2^{\mathcal{R}_n} &= \prod_{i=2}^{n} T_i^{\mathcal{R}_n[W_1]_i} \cdot \prod_{i=2}^{n} T_i^{\mathcal{R}_n[W_2]_i} \\ &= \prod_{i=2}^{n} T_i^{\mathcal{R}_n[W_1]_i +_2 \mathcal{R}_n[W_2]_i} \\ &= \prod_{i=2}^{n} T_i^{\overline{\mathcal{R}_n[W_1]_i +_2 \mathcal{R}_n[W_2]_i}}. \end{aligned}$$

It follows from Theorem 4.1 in [9], that

$$\mathcal{R}_n[W_1 \cdot W_2]_i = \mathcal{R}_n[W_1]_i +_2 \mathcal{R}_n[W_2]_i \ (i = 2, \ldots, n)$$

or

$$\mathcal{R}_n[W_1 \cdot W_2]_i = \overline{\mathcal{R}_n[W_1]_i +_2 \mathcal{R}_n[W_2]_i} \ (i = 2, \ldots, n).$$

Hence,

$$W_1^{\mathcal{R}_n} \cdot W_2^{\mathcal{R}_n} = \prod_{i=1}^{n} T_i^{\mathcal{R}_n[W_1 \cdot W_2]_i} = (W_1 \cdot W_2)^{\mathcal{R}_n},$$

as required. □

We call a word $W \in \mathcal{A}^{\sigma(n)}$ a *fixed word* of the mapping $.^{\mathcal{R}_n}$ if $W^{\mathcal{R}_n} = W$. Their set is denoted by $\mathcal{F}_n$. Proposition 2.3 implies that the word set $\mathcal{F}_n$ is a group. Furthermore, $\mathcal{R}_n \subseteq \mathcal{F}_n$, so we have $\langle \mathcal{R}_n \rangle \subseteq \mathcal{F}_n$, and, consequently,

THEOREM 2.3. *Let $n = 4, 8, \ldots$. Then, $\langle \mathcal{R}_n \rangle = \mathcal{F}_n$.* □

Specially, the cardinality of the word set $\mathcal{F}_n$, $|\mathcal{F}_n| = 2^{n-2}$ for $n = 4, 8, \ldots$, and the maximum cardinality of a multiplically independent word system in $\mathcal{F}_n$ (as in $\mathcal{R}_n$, too) is $n - 2$. This fact will be used in the proof of our main result in Section 4.

3 The symmetricity product of $\mathcal{R}_n$ and $[\langle \mathcal{R}_n \rangle]$

Our aim in this section is to simplify the proofs of Theorems 3.1 and 3.2 in [9], based on the results of Section 2.

Let us begin with a simple observation.

LEMMA 3.1. *The mapping $W \mapsto \mathcal{R}_n[W]$ is a bijection between the sets $\mathcal{F}_n$ and $\mathcal{R}_n[\mathcal{F}_n]$, for $n = 4, 8, \ldots$.*

Proof. The statement follows from the definition of fixed words: if $\mathcal{R}_n[W_1] = \mathcal{R}_n[W_2]$, then $W_1^{\mathcal{R}_n} = W_2^{\mathcal{R}_n}$, and so $W_1 = W_2$, for any $W_1, W_2 \in \mathcal{F}_n$. □

We will need also the following property of 0-1 vectors. Here $\mathbf{1}$ denotes the vector with all elements equal to one.

LEMMA 3.2. *Let $n = 4, 8, \ldots$. Then, the cardinality of the set of vectors $v \in \{0,1\}^n$ satisfying $\mathbf{1}^T v \equiv 3 \pmod 4$, is 2^{n-2}.*

Proof. First, note that the sets

$$\begin{aligned} V_1 &:= \{v \in \{0,1\}^n : \mathbf{1}^T v \equiv 3 \pmod 4\}, \\ V_2 &:= \{v \in \{0,1\}^n : \mathbf{1}^T v \equiv 1 \pmod 4\} \end{aligned}$$

have the same cardinality, as the negation is a bijection between them. Let $V := V_1 \cup V_2$, that is let

$$V := \{v \in \{0,1\}^n : \mathbf{1}^T v \equiv 1 \pmod 2\}.$$

By Exercise 1.42 a) in [3], we have

$$|V| = |\{0,1\}^n \setminus V| = 2^{n-1}.$$

Consequently, the cardinality of V_1, $|V_1| = 2^{n-2}$, the proof is finished. □

In the following we will prove the equation

$$\mathcal{R}_n[\mathcal{F}_n] = \{v \in \{0,1\}^n : \mathbf{1}^T v \equiv 3 \pmod 4\} \tag{1}$$

for $n = 4, 8, \ldots$. By Lemmas 3.1 and 3.2 the cardinalities of these two sets are equal (see also the remark made at the end of Section 2). Hence, to prove (1), it is enough to prove the inclusion

$$\mathcal{R}_n[\mathcal{F}_n] \subseteq \{v \in \{0,1\}^n : \mathbf{1}^T v \equiv 3 \pmod 4\} \tag{2}$$

for $n = 4, 8, \ldots$.

In [9] we have proved already the following two lemmas (weakenings of Lemma 3.1 resp. Theorems 3.1 and 3.2 in [9]).

LEMMA 3.3. *It holds that*

$$\mathcal{R}_n[\mathcal{A}^{\sigma(n)}] \subseteq \left\{ v \in \{0,1\}^n \;\middle|\; \mathbf{1}^T v = \begin{cases} 1 \text{ or } 3, & \text{if } n = 4, \\ 3 \text{ or } 7, & \text{if } n = 8, \\ 0, 3, 4, 7, \text{ or } 8, & \text{if } n = 9 \end{cases} \right\}.$$

Furthermore, in the case $n = 9$, $v = \mathcal{R}_n[W]$, $W \in \mathcal{A}^4$, *the equalities* $\mathbf{1}^T v = 0, 3, 4, 7$, *and* 8 *imply that* $bdbd[W] = 0, 1, 0, 1$, *and* 0, *respectively.*

LEMMA 3.4. *It holds that*

a) $\mathcal{R}_n[\mathcal{A}^{\sigma(n)}] \subseteq \{v \in \{0,1\}^n : \mathbf{1}^T v \equiv 1 \pmod 2\}$ $(n = 4, 12, \ldots)$;

b) $\mathcal{R}_n[\mathcal{A}^{\sigma(n)}] \subseteq \{v \in \{0,1\}^n : \mathbf{1}^T v \equiv 3 \pmod 4\}$ $(n = 8, 16, \ldots)$.

Now, we can derive the main result of this section.

THEOREM 3.1. *The equation (1) holds for* $n = 4, 8, \ldots$.

Proof. It is enough to verify the inclusion (2) for $n = 4, 8, \ldots$.

The case when $n = 8, 16, \ldots$ is a consequence of part b) of Lemma 3.4, as in this case, by Theorems 2.2 and 2.3, we have $\mathcal{F}_n = \mathcal{A}^{\sigma(n)}$.

The case when $n = 4, 12, \ldots$ can be proved by induction based on the definition of $\mathcal{R}_n$. For $n = 4$ the inclusion (2) is obvious. For the $n \to n + 8$ step let us suppose indirectly (see also part a) of Lemma 3.4) that there exists a word $W \in \mathcal{F}_{n+8}$ such that for the vector $v := \mathcal{R}_{n+8}[W]$, $\mathbf{1}^T v \equiv 1 \pmod 4$. Let us partition the word as $W =: W_S \& W_T$, where $W_S \in \mathcal{A}^4$, $W_T \in \mathcal{F}_n$ (see also Theorems 2.1 and 2.3). We have to deal with four cases:

Case 1: $T_1[W_T] = 0$ and $bdbd[W_S] = 0$;

Case 2: $T_1[W_T] = 0$ and $bdbd[W_S] = 1$;

Case 3: $T_1[W_T] = 1$ and $bdbd[W_S] = 0$;

Case 4: $T_1[W_T] = 1$ and $bdbd[W_S] = 1$.

Let us consider for example Case 1. Then, by the inductional assumption and $T_1[W_T] = 0$, we have

$$T_2[W_T] + \ldots + T_n[W_T] \equiv 3 \pmod 4.$$

Taking into account that $bdbd[W_S] = 0$, we obtain

$$bdbd\&T_2[W] + \ldots + bdbd\&T_n[W] \equiv 3 \pmod 4.$$

By the indirect assumption we can see that

$$S_1\&T_1[W] + \ldots + S_9\&T_1[W] \equiv 2 \pmod 4.$$

In other words (as $T_1[W_T] = 0$),

$$S_1[W_S] + \ldots + S_9[W_S] \equiv 2 \pmod 4,$$

contradicting Lemma 3.3. In this case the inclusion (2) is verified.

The Cases 2, 3, and 4 can be dealt with similarly, their proof is omitted. This concludes the proof of the theorem. □

To derive Theorems 3.1 and 3.2 in [9] as a consequence of Theorem 3.1 we will need the following two lemmas concerning the case $n = 4, 12, \ldots$.

LEMMA 3.5. *Let $n = 4, 12, \ldots$. Then, every word $W \in \mathcal{A}^{\sigma(n)}$ can be written uniquely as $W = W_1 \cdot W_2$ where $W_1 \in \mathcal{F}_n$, $W_2 \in \{a\}^{\sigma(n)-2} \& \{aa, ab, bc, bd\}$.*

Proof. The statement is an immediate consequence of Theorems 2.1 and 2.3. □

LEMMA 3.6. *Let $n = 4, 12, \ldots$. Then, $W_1 \in \mathcal{F}_n$, $W_2 \in \{a\}^{\sigma(n)-2} \& \{ab, bc, bd\}$ implies*

$$\mathcal{R}_n[W_1 \cdot W_2] = \overline{\mathcal{R}_n[W_1]}.$$

Proof. We use induction based on the definition of $\mathcal{R}_n$. The case when $n = 4$ is obvious. For the $n \to n+8$ step let us partition the considered words into two parts: let $W_1 =: W_S \& W_T$, where $W_S \in \mathcal{A}^4$, $W_T \in \mathcal{A}^{\sigma(n)}$. Similarly, let $W_2 =: W'_S \& W'_T$. Then,

$$\begin{aligned} \mathcal{R}_{n+8}[W_1 \cdot W_2] &= (\mathcal{R}_{n+8})_S[W_S \cdot W'_S] +_2 (\mathcal{R}_{n+8})_T[W_T \cdot W'_T] \\ &= (\mathcal{R}_{n+8})_S[W_S] +_2 \overline{(\mathcal{R}_{n+8})_T[W_T]} \\ &= \overline{\mathcal{R}_{n+8}[W_1]} \end{aligned}$$

using the inductional assumption and the fact that (by Theorems 2.1 and 2.3) $W_T \in \mathcal{F}_n$. □

Now, we can derive Theorems 3.1 and 3.2 in [9], with simplified proof.

THEOREM 3.2. *It holds that*

$$\mathcal{R}_n[\mathcal{A}^{\sigma(n)}] = \left\{ v \in \{0,1\}^n : \mathbf{1}^T v \equiv 1 \pmod 2 \right\},$$

for all $n \equiv 4 \pmod 8$.

Proof. It is enough to notice that by Lemmas 3.5 and 3.6 we have

$$\mathcal{R}_n[\mathcal{A}^{\sigma(n)}] = \mathcal{R}_n[\mathcal{F}_n] \cup \left\{ \overline{\mathcal{R}_n[W]} : W \in \mathcal{F}_n \right\}.$$

Then, the statement follows from Theorem 3.1. □

THEOREM 3.3. *It holds that*

$$\mathcal{R}_n[\mathcal{A}^{\sigma(n)}] = \left\{ v \in \{0,1\}^n : \mathbf{1}^T v \equiv 3 \pmod 4 \right\},$$

for all $n \equiv 0 \pmod 8$. *Furthermore, the mapping* $W \mapsto \mathcal{R}_n[W]$ *is a bijection between the sets* $\mathcal{A}^{\sigma(n)}$ *and* $\mathcal{R}_n[\mathcal{A}^{\sigma(n)}]$.

Proof. The statement follows from Theorem 3.1 and Lemma 3.1, as in the case when $n \equiv 0 \pmod 8$, by Theorems 2.2 and 2.3, we have the equation $\mathcal{F}_n = \mathcal{A}^{\sigma(n)}$. □

In the next section Theorem 3.1 will be applied in the proof of our main result.

4 Analogon of the Hadamard conjecture

In this section we will prove Theorem 1.4, even in a more general form.

Let us recall that in [9] $\hat{\mathcal{H}}_n$ denoted the set of words $W \in \mathcal{A}^{\sigma(n)}$ such that the words $a \dots a$ and W are orthogonal to each other. (Two words $W_1, W_2 \in \mathcal{A}^{\sigma(n)}$ are called *orthogonal* if the vectors $2\mathcal{R}_n[W_1] - \mathbf{1}, 2\mathcal{R}_n[W_2] - \mathbf{1} \in \{\pm 1\}^n$ are orthogonal to each other.) Let us denote by $\hat{\mathcal{H}}'_n$ the set of fixed words from the word set $\hat{\mathcal{H}}_n$, that is let $\hat{\mathcal{H}}'_n := \hat{\mathcal{H}}_n \cap \mathcal{F}_n$.

By Lemma 5.2 in [9],

$$\hat{\mathcal{H}}_n = \left\{ W \in \mathcal{A}^{\sigma(n)} \,\middle|\, \mathbf{1}^T \mathcal{R}_n[W] = \left\{ \begin{array}{ll} n/2 - 1, & \text{if } (\mathcal{R}_n[W])_1 = 0, \\ n/2 + 1, & \text{if } (\mathcal{R}_n[W])_1 = 1 \end{array} \right\} \right.,$$

which implies, using Theorem 3.1, the formulas

$$\begin{aligned} \hat{\mathcal{H}}'_n &= \{W \in \mathcal{F}_n : \mathbf{1}^T \mathcal{R}_n[W] = n/2 + 1,\ \mathcal{R}_n[W]_1 = 1\} \ (n = 4, 12, \dots), \\ \hat{\mathcal{H}}'_n &= \{W \in \mathcal{F}_n : \mathbf{1}^T \mathcal{R}_n[W] = n/2 - 1,\ \mathcal{R}_n[W]_1 = 0\} \ (n = 8, 16, \dots). \end{aligned}$$

We can see, by Lemma 3.1,

THEOREM 4.1. *The mapping* $W \mapsto \mathcal{R}_n[W]$ *is a bijection between the sets* $\hat{\mathcal{H}}'_n$ *and* V, *where*

a) $V = \{v \in \{0,1\}^n : \mathbf{1}^T v = n/2 + 1,\ v_1 = 1\}$, *if* $n = 4, 12, \dots$;

b) $V = \{v \in \{0,1\}^n : \mathbf{1}^T v = n/2 - 1,\ v_1 = 0\}$, *if* $n = 8, 16, \dots$.

Specially, the cardinality of the word set $\hat{\mathcal{H}}'_n$ *is*

$$|\hat{\mathcal{H}}'_n| = \left(\begin{array}{c} n-1 \\ \frac{n}{2} - 1 \end{array} \right),$$

if $n = 4, 8, \dots$. □

There is another approach showing, too, the multitude of the elements in $\hat{\mathcal{H}}'_n$. (Here $\mathcal{W}_1 \cdot \mathcal{W}_2$ denotes the set of words of the form $W_1 \cdot W_2$, $W_1 \in \mathcal{W}_1$, $W_2 \in \mathcal{W}_2$, for arbitrary word sets $\mathcal{W}_1, \mathcal{W}_2 \subseteq \mathcal{A}^{\sigma(n)}$.)

THEOREM 4.2. *Let* $n = 4, 8, \ldots$. *Then,* $\hat{\mathcal{H}}'_n \cdot \hat{\mathcal{H}}'_n = \mathcal{F}_n$.

Proof. Let us consider for example the case when $n = 4, 12, \ldots$, the case when $n = 8, 16, \ldots$ can be dealt with similarly. Let $W \in \mathcal{F}_n$, then, by Proposition 2.1,

$$W = \prod_{i=2}^{n} T_i^{\mathcal{R}_n[W]_i} = \prod_{i=2}^{n} T_i^{1-\mathcal{R}_n[W]_i}.$$

Two cases are possible (see Theorem 3.1):

1. $\mathcal{R}_n[W]_1 = 1$, then $\sum_{i=2}^{n} \mathcal{R}_n[W]_i = 2, 6, \ldots, n-2$;
2. $\mathcal{R}_n[W]_1 = 0$, then $\sum_{i=2}^{n} 1 - \mathcal{R}_n[W]_i = 0, 4, \ldots, n-4$.

Consequently,

$$W = \prod_{i=2}^{n} T_i^{\varepsilon_i}, \text{ where } \varepsilon_2 + \ldots + \varepsilon_n = 0, 2, \ldots, n-2.$$

We have to find words

$$W_1 = \prod_{i=2}^{n} T_i^{\mu_i},\ W_2 = \prod_{i=2}^{n} T_i^{\nu_i}$$

satisfying $W_1 \cdot W_2 = W$ and $W_1, W_2 \in \hat{\mathcal{H}}'_n$, that is (see Theorem 4.1)

$$\varepsilon_i = \mu_i +_2 \nu_i \ (i = 2, \ldots, n),\ \sum_{i=2}^{n} \mu_i = \sum_{i=2}^{n} \nu_i = n/2.$$

In other words, we have to find sets of indices

$$N_{00} := \{i : \mu_i = 0,\ \nu_i = 0\}, \qquad N_{11} := \{i : \mu_i = 1,\ \nu_i = 1\},$$
$$N_{01} := \{i : \mu_i = 0,\ \nu_i = 1\}, \qquad N_{10} := \{i : \mu_i = 1,\ \nu_i = 0\}$$

with cardinalities $n_{00}, n_{11}, n_{01}, n_{10}$ satisfying the equations

$$n_{00} + n_{01} + n_{10} + n_{11} = n - 1,$$
$$n_{01} + n_{11} = n/2 = n_{10} + n_{11},$$
$$n_{01} + n_{10} = 0, 2, \ldots, n-2.$$

It can be easily seen that such sets $N_{00}, N_{11}, N_{01}, N_{10}$ do exist, which completes the proof. □

Necessarily, $\hat{\mathcal{H}}'_n$ (as $\mathcal{F}_n$, too) can not be generated by less than $n-2$ words; there exist $n-2$ multiplically independent words in $\hat{\mathcal{H}}'_n$: We obtained a *proof of Theorem 1.4.* □

Obviously, similar statement holds with $a\ldots a^{\perp} = \hat{\mathcal{H}}'_n$ replaced with $W^{\perp} = W \cdot \hat{\mathcal{H}}'_n$ (see Lemma 5.2 in [9]), where $W^{\perp}$ denotes the set of fixed words orthogonal to the word $W \in \mathcal{F}_n$. Then $W^{\perp}$ is called a *hyperplane* of $\mathcal{F}_n$ with *normal word* $W \in \mathcal{F}_n$.

THEOREM 4.3. *Let $W \in \mathcal{F}_n$ be an arbitrary fixed word. Then, there exist words $W_1, \ldots, W_{n-2} \in \hat{\mathcal{H}}'_n$ such that the word system $W \cdot W_1, \ldots, W \cdot W_{n-2}$ is multiplically independent.* □

It is an open problem whether multiplical independence of a word system implies its linear independence, or not. (By *linear independence* of a word system $W_1, \ldots, W_m \in \mathcal{F}_n$ we mean that the vectors $2\mathcal{R}_n[W_1]-\mathbf{1}, \ldots, 2\mathcal{R}_n[W_m]-\mathbf{1} \in \{\pm 1\}^n$ are linearly independent.) We remark that a word system can be orthogonal without being multiplically independent, as the word system

$$aaa, acd, adc, caa, ccd, cdc, abb, cbb$$

shows: it is orthogonal, generated by the multiplically independent words *acd*, *adc*, *caa*.

Maximal multiplically independent word systems play a role similar to that of positive definite matrices in linear algebra: norms and induced scalar products, induced metrics of words (and, consequently, projection, that is nearest words in a given set of words to a given word, angle of two words, ... etc.) can be defined using them.

Indeed, let $\mathcal{P} \subseteq \mathcal{F}_n$ be a multiplically independent word system with $n-2$ elements $P_1, \ldots, P_{n-2}$. Let us define the $\mathcal{P}$-*norm* of a word $W \in \mathcal{F}_n$ as

$$||W||_{\mathcal{P}} := \sum_{i=1}^{n-2} \varepsilon_i, \text{ if } W = P_1^{\varepsilon_1} \cdot \ldots \cdot P_{n-2}^{\varepsilon_{n-2}}, \varepsilon_1, \ldots, \varepsilon_{n-2} \in \{0,1\}.$$

Then, let us define the $\mathcal{P}$-*scalar product* of two words $W_1, W_2 \in \mathcal{F}_n$ as

$$W_1 \bullet_{\mathcal{P}} W_2 := \frac{1}{2} \cdot \left(||W_1||_{\mathcal{P}}^2 + ||W_2||_{\mathcal{P}}^2 - ||W_1 \cdot W_2||_{\mathcal{P}}^2 \right).$$

Let us define also the $\mathcal{P}$-*distance* of two words $W_1, W_2 \in \mathcal{F}_n$ as

$$\varrho_{\mathcal{P}}(W_1, W_2) := ||W_1 \cdot W_2||_{\mathcal{P}}.$$

Note that $||W||_{\mathcal{P}} = 0$ if and only if $W = a \dots a$. Furthermore, $W \bullet_{\mathcal{P}} W = ||W||^2_{\mathcal{P}}$.

The following statements are immediate from the definition of the norm, scalar product, and distance of words.

PROPOSITION 4.1. *Let $\mathcal{P} \subseteq \mathcal{F}_n$ be a multiplically independent word system with $n-2$ elements. Then the inequalities*

a) $||W_1 \cdot W_2||_{\mathcal{P}} \leq ||W_1||_{\mathcal{P}} + ||W_2||_{\mathcal{P}}$,

b) $\pm(W_1 \bullet_{\mathcal{P}} W_2) \leq ||W_1||_{\mathcal{P}} \cdot ||W_2||_{\mathcal{P}}$,

c) $\varrho_{\mathcal{P}}(W_1, W_2) \leq \varrho_{\mathcal{P}}(W_1, W_3) + \varrho_{\mathcal{P}}(W_3, W_2)$

hold, for any words $W_1, W_2, W_3 \in \mathcal{F}_n$. □

We hope that these notions will be useful in the construction and analysis of a Gram-Schmidt-type algorithm (see [5]) which starting with a multiplically independent word system with $n-2$ elements in $\hat{\mathcal{H}}'_n$, calculated the usual greedy way, produces in finite number of steps an orthogonal word system with $n-2$ elements in $\hat{\mathcal{H}}'_n$, and thus (by Theorem 1.3) settles the Hadamard conjecture for $n = 4k$, $k = 1, 2, \dots$.

Conclusion. In the paper we proved an analogon of the linear algebraic theorem that each hyperplane of an n-dimensional Euclidean space contains $n-1$ linearly independent vectors. Our main result states that each hyperplane of fixed words is of the same multiplical dimension as the space of fixed words. This result is a counterpart of Tressler's Theorem on Hadamard matrices. Some refinements and simplified proofs of results concerning image vectors, from a previous work of the author, were also described.

References

1. SZ. V. Jablonszkij and O. B. Lupanov, *Discrete mathematics in computer science*, Műszaki Könyvkiadó, Budapest, 1980 (in Hungarian).

2. H. Kharaghani and B. Tayfeh-Rezaie, *A Hadamard matrix of order 428*, J. Combin. Des. 13 (2005), 435-440.

3. L. Lovász, *Combinatorial problems and exercises*, Akadémiai Kiadó, Budapest, 1979.

4. R. E. A. C. Paley, *On orthogonal matrices*, Journal of Mathematics and Physics 12 (1933), 311-320.

5. G. Strang, *Linear algebra and its applications*, Academic Press, New York, 1980.

6. J. J. Sylvester, *Thoughts on inverse orthogonal matrices, simultaneous sign successions, and tessellated pavements in two or more colours, with applications to Newton's rule, ornamental tile-work, and the theory of numbers*, Philosophical Magazine 34 (1867), 461-475.

7. E. Tressler, *A survey of the Hadamard conjecture*, M. S. thesis submitted to Virginia Polytechnic Institute and State University, Blacksburg, Virginia, 2004.

8. M. Ujvári, *New descriptions of the Lovász number, and the weak sandwich theorem*, submitted to Pure Math. Appl. (2010).

9. M. Ujvári, *Reformulation of the Hadamard conjecture via Hurwitz-Radon word systems*, submitted to Pure Math. Appl. (2010).

Miklós Ujvári
H-2600 Vác, Szent János utca 1. HUNGARY

Recent Operations Research Reports

2005-03 Bilen Filiz, Zsolt Csizmadia and Tibor Illés : Anstreicher-Terlaky type monotonic simplex algorithms for linear feasibility problems

2005-04 Tibor Illés, Márton Makai, Zsuzsanna Vaik: Railway Engine Assignment Models Based on Combinatorial and Integer Programming

2006-01 Miklós Ujvári: Simplex-type algorithm for optimizing a pseudolinear quadratic fractional function over a polytope

2006-02 Miklós Ujvári: New descriptions of the Lovász number and a Brooks-type theorem

2007-01 Miklós Ujvári: On Abrams' theorem

2007-02 Tibor Illés, Marianna Nagy, Tamás Terlaky: An EP theorem for dual linear complementarity problem

2007-03 Tibor Illés, Marianna Nagy, Tamás Terlaky: Polynomial interior point algorithms for general LCPs

2009-01 Miklós Ujvári: On closedness conditions, strong separation, and convex duality

2009-02 Miklós Ujvári: Reformulation of the Hadamard conjecture via Hurwitz-Radon word systems

2010-01 Miklós Ujvári: Strengthening weak sandwich theorems in the presence of inconnectivity

2010-02 Tibor Illés, Zsolt Csizmadia: The s-Monotone Index Selection Rules for Pivot Algorithms of Linear Programming

2010-03 Miklós Ujvári: Four new upper bounds for the stability number of a graph

2011-01 Miklós Ujvári: Applications of the inverse theta number in stable set problems