Counterpart results in word spaces

Miklós Ujvári *

Abstract. In this paper after algebraical and geometrical preliminaries we present a Gram–Schmidt-type algorithmical conjecture, which if true settles the long-standing Hadamard conjecture concerning the existence of orthogonal matrices with elements of the same absolute value.

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

1 Introduction

A matrix $H \in \{\pm 1\}^{n\times r}$ (resp. $M \in \{0,1\}^{n\times r}$) is called an *Hadamard matrix* if

$$H^*H = nI \text{ (resp. } (2M-J)^*(2M-J) = nI),$$

where $*$ denotes transpose, I is the identity matrix, and J is the matrix with all elements equal to 1. The *Hadamard conjecture* states that an Hadamard matrix (either in $\{\pm 1\}^{n\times r}$ or $\{0,1\}^{n\times r}$) exists if and only if (r,n) satisfies one of the following requirements:

a) $r = 1$, n arbitrary;

b) $r = 2$, n even;

c) $3 \le r \le n$, n divisible by 4.

It is easy to verify that the nontrivial part of the Hadamard conjecture is the existence of an Hadamard matrix $M \in \{0,1\}^{n\times n}$ for all n divisible by 4. The latter statement is proved for all $n < 668$ (see [2]), and for some infinite classes of n, see [5], [3]. For a historical overview we refer to [1], [6].

We start this paper by describing a possible way of reducing the problem size, see [7], [8].

A basic result concerning Hadamard matrices in $\{0,1\}^{n\times n}$ is Tressler's theorem, see [6]. (Here $+_2$ denotes the elementwise addition modulo 2 on $\{0,1\}^{n\times r}$.)

THEOREM 1.1. (Tressler) *Let $n = 4, 8, \ldots$. Then, the following statements hold:*

a) If $M' \in \{0,1\}^{n\times(n-1)}$ is an Hadamard matrix, then there exists an Hadamard matrix $M \in \{0,1\}^{n\times n}$ such that M' is a submatrix of M;

*H-2600 Vác, Szent János utca 1. HUNGARY

b) If $M \in \{0,1\}^{n\times n}$ is an Hadamard matrix, then the $+_2$-sum of its column vectors is either (0) *or* (1).

Consequently, it suffices to search for an Hadamard matrix $M \in \{0,1\}^{n\times(n-1)}$. Let us suppose that we have found such a matrix M. As the negation of rows and columns of M does not change the property of its being an Hadamard matrix, so it is easy to see that we can assume that in M:

a) the first column vector is $(0,1,\ldots,1)^*$;

b) the first row vector is $(0,1,\ldots,1)$ if $n = 4, 12, \ldots$;

c) the first row vector is $(0,0,\ldots,0)$ if $n = 8, 16, \ldots$.

Then, the matrix M has its columns in the set

$$V := \left\{ v = (v_i) \in \{0,1\}^n : \sum_{i=1}^{n} v_i \equiv 3 \pmod 4 \right\}.$$

Note that the search for M is simplified: the cardinality of V is $\#V = 2^{n-2}$ only, which is a quarter of the cardinality of $\{0,1\}^n$, where we worked so far.

In [8], the vectors in V are labeled bijectively with the *fixed words* in $\mathcal{F}_n \subseteq \mathcal{A}^{\sigma(n)}$,

$$\mathcal{F}_n := \{W \in \mathcal{A}^{\sigma(n)} : \ell(\ell^{-1}(W)) = W\},$$

where the alphabet $\mathcal{A}$ consists of the letters a, b, c, d, and $\sigma(n)$ denotes

$$\sigma(n) := \begin{cases} n/2, & \text{if } n = 4, 12, \ldots, \\ n/2 - 1, & \text{if } n = 8, 16, \ldots. \end{cases}$$

The bijective *labeling* map $\ell : V \to \mathcal{F}_n$ is

$$\ell : (v_i) \mapsto \prod_{i=1}^{n} T_i^{v_i},$$

where $\mathcal{R}_n = (T_1, \ldots, T_n)$ is the *canonical word system* in $\mathcal{A}^{\sigma(n)}$ (see Section 2), and the *letterwise product* $\prod$ on $\mathcal{A}^{\sigma(n)}$ is induced by the multiplication table of a Klein group on $\mathcal{A}$:

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

The inverse of the labeling map, $\ell^{-1} : \mathcal{F}_n \to V$ is

$$\ell^{-1} : W \mapsto (T_i[W])_{i=1}^{n},$$

where $X[Y]$ denotes the *symmetricity product* of the words $X, Y \in \mathcal{A}^{\sigma(n)}$, that is the number of the letters b in the word $X \cdot Y$, taken modulo 2.

Appropriately defined, orthogonality of vectors translates into orthogonality of words, and vice versa.

Two vectors $v, w \in V$ are said to be *orthogonal* (to each other) if

$$(2v - (1))^*(2w - (1)) = 0.$$

Two words $X, Y \in \mathcal{F}_n$ are *orthogonal* (to each other) if $X \cdot Y \in \hat{\mathcal{H}}'_n$, where

$$\begin{aligned} \hat{\mathcal{H}}'_n &= \left\{ W \in \mathcal{F}_n : \sum_{i=1}^{n} T_i[W] = n/2 + 1,\ T_1[W] = 1 \right\}\ (n = 4, 12, \ldots), \\ \hat{\mathcal{H}}'_n &= \left\{ W \in \mathcal{F}_n : \sum_{i=1}^{n} T_i[W] = n/2 - 1,\ T_1[W] = 0 \right\}\ (n = 8, 16, \ldots). \end{aligned}$$

With these definitions the labeling ℓ and its inverse ℓ^{-1} have the following properties:

a) If $v, w \in V$ are orthogonal vectors, then $\ell(v), \ell(w) \in \mathcal{F}_n$ are orthogonal words;

b) If $X, Y \in \mathcal{F}_n$ are orthogonal words, then $\ell^{-1}(X), \ell^{-1}(Y) \in V$ are orthogonal vectors;

c) The so-called *trivial word* $T_1 \in \{a\}^{\sigma(n)}$ is the identity element of the group $(\mathcal{F}_n, \cdot)$. Specially, $\hat{\mathcal{H}}'_n$ consists of the fixed words orthogonal to T_1.

Summarizing, the *Hadamard conjecture* is further *reduced* to the problem of finding pairwise orthogonal words $W_1, \ldots, W_{n-2} \in \hat{\mathcal{H}}'_n$. Note that the cardinality of the word set $\hat{\mathcal{H}}'_n$ is

$$\#\hat{\mathcal{H}}'_n = \begin{pmatrix} n-1 \\ n/2-1 \end{pmatrix},$$

which means reduction of the problem size compared to $\#V = 2^{n-2}$.

A counterpart of this reduced form of the problem is dealt with in [8], where it is shown that there exist $n-2$ multiplically independent words in $\hat{\mathcal{H}}'_n$. (Here a word system $W_1, \ldots, W_r \in \mathcal{A}^{\sigma(n)}$ is called *multiplically independent* if

$$\left.\begin{array}{r} W_1^{\varepsilon_1} \cdot \ldots \cdot W_r^{\varepsilon_r} = T_1 \\ \varepsilon_1, \ldots, \varepsilon_r \in \{0, 1\} \end{array}\right\} \text{ implies } \varepsilon_1 = \ldots = \varepsilon_r = 0.$$

In other words, the system $W_1, \ldots, W_r \in \mathcal{A}^{\sigma(n)}$ is multiplically independent if and only if its *generated word set*,

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

is of cardinality 2^r.) A constructive proof will be given in Section 2.

The main aim of this paper is to describe an algorithmical conjecture (Section 4), which if true connects the existence of multiplically independent words to the existence of orthogonal words. While sudying the preliminary results (Sections 2 and 3) we underline continuously, that they always have a counterpart result of similar structure.

2 Orthogonality and independence

In this section we will prove algebraical results in word spaces.

Let us recall the inductive definition of the *canonical word system* $\mathcal{R}_n$ (see for example [7], [8]). 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 $\mathcal{R}_n$ for all $n \equiv 0, 1, 2, 4 \pmod 8$. Note that $(T_i[T_j]) = J - I$.

In what follows we will suppose that $n = 4, 8, \ldots$. We mention two basic properties of the canonical word system $\mathcal{R}_n$, see [8]:

$(P1)$: The letterwise product of the words in $\mathcal{R}_n$ is $\prod_{i=1}^{n} T_i = T_1$;

$(P2)$: Leaving out from $\mathcal{R}_n$ its first word T_1 and another word T_i, we obtain a multiplically independent word system $\mathcal{P}_i$ $(2 \le i \le n)$ with $n - 2$ elements in $\mathcal{F}_n = \langle \mathcal{P}_i \rangle$.

Proposition 2.1 describes a counterpart of $(P1)$:

PROPOSITION 2.1. *Let $W_1, \ldots, W_n \in \mathcal{F}_n$ be pairwise orthogonal words. Then, $W_1 \cdot \ldots \cdot W_n = T_1$ holds.*

Proof. As, obviously,

$$W_1 \cdot \ldots \cdot W_n = (W_1 \cdot W_1) \cdot \ldots \cdot (W_1 \cdot W_n),$$

so we can assume that $W_1 = T_1$. Furthermore, we will consider only the case when $n = 4, 12, \ldots$, as the complementer case $n = 8, 16, \ldots$ can be dealt with similarly.

Let us negate the first row vector in the matrix

$$(T_i[W_j]) \in \{0,1\}^{n\times n},$$

this way we obtain an Hadamard matrix $M \in \{0,1\}^{n\times n}$ whose first column vector is (1) and first row vector is $(1,0,\ldots,0)$. In the case of the matrix M, by Tressler's theorem, we have

$$m_n = m_2 +_2 \ldots +_2 m_{n-1},$$

where m_j denotes the j-th column vector of M. Hence,

$$\begin{aligned} W_2 \cdot \ldots \cdot W_n &= \prod_{j=2}^{n}\prod_{i=2}^{n} T_i^{T_i[W_j]} = \\ &= \prod_{i=2}^{n} T_i^{\sum_2 T_i[W_j]} = \prod_{i=2}^{n} T_i^0 = T_1, \end{aligned}$$

which completes the proof. □

As a consequence, we obtain a constructive proof of the fact (see Section 1) that in order to settle the Hadamard conjecture it suffices to find $n-2$ pairwise orthogonal words in $\hat{\mathcal{H}}'_n$ instead of $n-1$, a counterpart of $(P2)$.

PROPOSITION 2.2. *The pairwise orthogonality of the words $W_1,\ldots,W_{n-1} \in \mathcal{F}_n$ implies the pairwise orthogonality of the words $W_1,\ldots,W_n$, where the n-th (fixed) word is defined as $W_n := W_1 \cdot \ldots \cdot W_{n-1}$.*

Proof. As in the proof of Proposition 2.1, we will consider only the case when $W_1 = T_1$ and $n = 4, 12, \ldots$.

Let us negate the first row vector in the matrix

$$(T_i[W_j]) \in \{0,1\}^{n\times(n-1)},$$

and denote the Hadamard matrix obtained this way by M'. Then, the column vectors in M' are $m'_1 = (1)$, and $m'_2,\ldots,m'_{n-1}$ with first element 0. By Tressler's theorem, the matrix

$$M := (M', m_n) \in \{0,1\}^{n\times n},$$

where

$$m_n := m'_2 +_2 \ldots +_2 m'_{n-1},$$

is an Hadamard matrix. Negating the first element of its n-th column vector m_n we obtain a vector in V, necessarily of the form $(T_i[W])$ for some $W \in \mathcal{F}_n$. Then, the words $W_1,\ldots,W_{n-1},W \in \mathcal{F}_n$ are pairwise orthogonal (their images at ℓ^{-1} are the column vectors of an Hadamard matrix). From Proposition 2.1 we obtain $W = W_n$, which was to be shown. □

Our next aim is to describe a counterpart of the reduced form of the Hadamard conjecture (see Section 1). We need an equivalent description of the word set $\hat{\mathcal{H}}'_n$, which is based on

LEMMA 2.1. *Let us suppose that* $W = \prod_{i=2}^{n} T_i^{\varepsilon_i}$ *for some* $\varepsilon_i \in \{0,1\}$, $i = 2,\dots,n$. *Then, either* $\varepsilon_i = T_i[W]$ *for all* i, *or* $\varepsilon_i = 1 - T_i[W]$ *for all* i.

Proof. The case when $\varepsilon_i = 1$ for all i is obvious, see $(P1)$. Hence, we can suppose that $\varepsilon_{i_0} = 0$ for some index i_0, and, for example, $T_{i_0}[W] = 0$ (if $T_{i_0}[W] = 1$ then we can substitute $T_i[W]$ with $1 - T_i[W]$ for $i = 2,\dots,n$ in the argument). Then, as $W \in \mathcal{F}_n$, so

$$W = \prod_{i \neq i_0} T_i^{\varepsilon_i} = \prod_{i \neq i_0} T_i^{T_i[W]}$$

holds. By $(P2)$ the word set $\mathcal{P}_{i_0}$ is multiplically independent, so we have $\varepsilon_i = T_i[W]$ $(i \neq i_0)$, as well as $\varepsilon_{i_0} = T_{i_0}[W] = 0$, which is the desired conclusion. □

Now, we can derive easily the following useful description of $\hat{\mathcal{H}}'_n$.

THEOREM 2.1. *Let us suppose that* $W = \prod_{i=2}^{n} T_i^{\varepsilon_i}$ *for some* $\varepsilon_i \in \{0,1\}$, $i = 2,\dots,n$. *Then,* $W \in \hat{\mathcal{H}}'_n$ *if and only if* $\sum_{i=2}^{n} \varepsilon_i = n/2$ *or* $n/2 - 1$.

Proof. Let us consider for example the case when $n = 4, 12, \dots$, the case when $n = 8, 16, \dots$ can be dealt with similarly.

The "only if" part is an immediate consequence of Lemma 2.1. In the "if" part, by Lemma 2.1,

$$\sum_{i=2}^{n} T_i[W] = n/2 \text{ or } n/2 - 1$$

holds. As $\ell^{-1}(W) \in V$, so the latter case can be excluded, and also $T_1[W] = 1$. By definition, $W \in \hat{\mathcal{H}}'_n$ follows, completing the "if" part of the proof. □

The counterpart of the reduced Hadamard conjecture concerns maximal multiplically independent word systems in $\hat{\mathcal{H}}'_n$.

Let us define $n-2$ words $B_1,\dots,B_{n-2}$ in $\mathcal{F}_n$ as follows: multiply $n/2-1$ ($n/2$ times) resp. $n/2$ ($n/2-2$ times) consecutive words from the system $(\mathcal{P},\mathcal{P})$ (with $\mathcal{P}$ as in $(P2)$) starting the multiplication at the first, second, ... , resp. $(n-2)$-th word of the system $(\mathcal{P},\mathcal{P})$. The word system

$$\mathcal{B}_{\mathcal{P}} := (B_1,\dots,B_{n-2})$$

obtained this way is called the *bearded-*$\mathcal{P}$ word system. For example, for $n = 8$,

$$\mathcal{B}_{\mathcal{P}_n} = (caa, bcb, ada, bbd, acc, bbc) \subseteq \hat{\mathcal{H}}'_n,$$

where the inclusion follows from the fact that $\hat{\mathcal{H}}'_8$ equals the set of nontrivial 3-letter words containing zero or two of the letter b.

THEOREM 2.2. *Let $\mathcal{P} := \mathcal{P}_i$ denote a subsystem of $\mathcal{R}_n$ with $n-2$ nontrivial elements, as in $(P2)$. Then, the bearded-$\mathcal{P}$ word system $\mathcal{B} := \mathcal{B}_\mathcal{P}$ consists of $n-2$ words from $\hat{\mathcal{H}}'_n$, and it is multiplically independent.*

Proof. The first assertion $\mathcal{B} \subseteq \hat{\mathcal{H}}'_n$ follows by Theorem 2.1.

In order to prove the multiplical independence of $\mathcal{B}$ we transform $\mathcal{B}$ into another word system $\mathcal{B}'$ such that its multiplical (in)dependence is preserved. To this end multiply the word $B_{n/2+i}$ in $\mathcal{B}$ by the word $B_1 B_{n/2} B_{i+1}$ $(1 \leq i \leq n/2-2)$. (The words $B_1, \ldots, B_{n/2}$ in $\mathcal{B}$ remain unchanged.) The word system $\mathcal{B}'$ obtained this way (via a number of elementary transformations) obviously meets the requirements. On the other hand, it can easily be verified that the word system $\mathcal{B}'$ is multiplically independent. Hence, the same holds for the bearded word system $\mathcal{B}$, too; the proof is finished. □

It is known (see [8], Theorem 4.3) that the word set

$$X \cdot \hat{\mathcal{H}}'_n := \{X \cdot Z : Z \in \hat{\mathcal{H}}'_n\} \ (X \in \mathcal{F}_n)$$

contains $n-2$ multiplically independent words, but it is an open problem to find a constructive proof of this fact (Theorem 2.2 deals with the special case, when $X = T_1$).

3 Hyperplanes

In this section we will study geometrical results in the word spaces.

The word set $X \cdot \hat{\mathcal{H}}'_n$ consists of the fixed words orthogonal to the word $X \in \mathcal{F}_n$. It is also denoted by $X^\perp$, and is called a *hyperplane* with *normal word* X. Specially, $T_1^\perp = \hat{\mathcal{H}}'_n$.

Any hyperplane has a unique normal word; we will prove this result (Theorem 3.1) adapting the technique used in the proof of its counterpart, the equalities

$$\mathcal{F}_n = \cup\{Z^\perp : Z \in X^\perp\} \ (X \in \mathcal{F}_n) \tag{1}$$

(Theorem 4.2 in [8]). Note that (1) claims that for each word pair $X, Y \in \mathcal{F}_n$ the hyperplanes $X^\perp$ and $Y^\perp$ intersect (as $Y \in Z^\perp$ means $Z \in Y^\perp$).

THEOREM 3.1. *Let $X, Y \in \mathcal{F}_n$ be different fixed words. Then, the hyperplanes $X^\perp, Y^\perp \subseteq \mathcal{F}_n$ differ, too.*

Proof. To prove the assertion we have to find a word $Z \in \mathcal{F}_n$ such that

$$X \cdot Z \in \hat{\mathcal{H}}'_n \not\ni Y \cdot Z. \tag{2}$$

Obviously, we can suppose that $Y = T_1$. (If this would not be the case, then consider $X \cdot Y$ and T_1 instead of X and Y, respectively.)

Let us write the words X, Z as

$$X = \prod_{i=2}^{n} T_i^{\xi_i},\ Z = \prod_{i=2}^{n} T_i^{\zeta_i},$$

and define the index sets

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

with cardinalities $n_{00}, n_{11}, n_{01}, n_{10}$, respectively. We are given the word $X \neq T_1$, which means that the sum $n_{10} + n_{11}$ is a given positive integer. We can suppose that $n_{10} + n_{11}$ is even, as we can substitute ξ_i with $1 - \xi_i$ for $i = 2, \ldots, n$, if necessary (see $(P2)$ and $(P1)$).

To find an appropriate word Z in (2), we have to solve the following inequality system (see Theorem 2.1):

$$n_{10} + n_{11} = 2, 4, \ldots, n-2.$$
$$n_{10} + n_{01} = n/2,$$
$$n_{11} + n_{01} \neq n/2, n/2 - 1$$
$$n_{10} + n_{01} + n_{11} \leq n - 1.$$

It can easily be seen that such a solution n_{01}, n_{10}, n_{11} always exists, which completes the proof. □

Equivalently, with the notation

$$X^{\perp\perp} = \cap\{Z^{\perp} : Z \in X^{\perp}\}\ (X \in \mathcal{F}_n),$$

we have

COROLLARY 3.1. *For any $X \in \mathcal{F}_n$,*

$$X^{\perp\perp} = \{X\} \tag{3}$$

holds.

Proof. Let $Y \in X^{\perp\perp}$, then $Y^{\perp} \supseteq X^{\perp}$ holds. As $Y^{\perp}$ and $X^{\perp}$ have the same cardinality, so $Y^{\perp} = X^{\perp}$ follows. Applying Theorem 3.1, we reach the desired conclusion $Y = X$. □

We remark that while (1) states that any two words is contained in a hyperplane, by Corollary 3.1 the orthogonal complement of a hyperplane does not contain any two words.

Now, we describe an extension of Corollary 3.1. Let us denote

$$(X, Y)^{\perp\perp} = \cap\{Z^{\perp} : Z \in X^{\perp} \cap Y^{\perp}\}$$

for $X, Y \in \mathcal{F}_n$. Similarly, as in the special case $X = Y$, we have

THEOREM 3.2. *Let $X, Y \in \mathcal{F}_n$ be arbitrary fixed words. Then,*

$$(X, Y)^{\perp\perp} = \{X, Y\} \tag{4}$$

holds.

Proof. Without loss of generality assuming $Y = T_1$, we have to prove that

$$(\forall W \in \mathcal{F}_n \setminus \{T_1, X\})\ (\exists Z \in T_1^{\perp} \cap X^{\perp})\ WZ \notin T_1^{\perp}. \tag{5}$$

Let us introduce the notation $\varepsilon_i, \xi_i, \zeta_i \in \{0, 1\}$ $(2 \le i \le n)$ so that

$$W = \prod_{i=2}^{n} T_i^{\varepsilon_i},\ X = \prod_{i=2}^{n} T_i^{\xi_i},\ Z = \prod_{i=2}^{n} T_i^{\zeta_i},$$

and also $2 \le \kappa, \lambda \le n-2$, $0 \le \mu \le n-2$ even integers such that

$$\kappa := \sum_{i=2}^{n} \varepsilon_i,\ \lambda := \sum_{i=2}^{n} (\varepsilon_i +_2 \xi_i),\ \mu := \sum_{i=2}^{n} \xi_i$$

satisfy

$$\kappa + \lambda \ge \mu,\ \kappa + \mu \ge \lambda,\ \lambda + \mu \ge \kappa,\ \kappa + \lambda + \mu \le 2n - 2.$$

Similarly as in Theorem 3.1 we can see that in order to prove (5) it suffices to solve the inequality system

$$\begin{aligned}
e_1 &: \quad n_{100} + n_{101} + n_{110} + n_{111} = \kappa,\\
e_2 &: \quad n_{010} + n_{011} + n_{100} + n_{101} = \lambda,\\
e_3 &: \quad n_{001} + n_{011} + n_{101} + n_{111} = n/2,\\
e_4 &: \quad n_{001} + n_{010} + n_{101} + n_{110} = n/2,\\
e_5 &: \quad n_{010} + n_{011} + n_{110} + n_{111} = \mu,\\
e_6 &: \quad n_{001} + n_{011} + n_{100} + n_{110} \ne n/2, n/2 - 1,\\
e_7 &: \quad \sum_{\varepsilon\xi\zeta \ne 000} n_{\varepsilon\xi\zeta} \le n - 1,\ n_{001}, \ldots, n_{111} \ge 0,
\end{aligned}$$

where as usual

$$N_{\varepsilon\xi\zeta} := \{i : \varepsilon_i = \varepsilon,\ \xi_i = \xi,\ \zeta_i = \zeta\},\ n_{\varepsilon\xi\zeta} := \#N_{\varepsilon\xi\zeta}$$

for $\varepsilon, \xi, \zeta \in \{0, 1\}$. After some obvious manipulations

$$\begin{gathered}
2e_1' := (e_1 - e_2) - (e_3 - e_4),\ 2e_1'' := (e_1 - e_2) + (e_3 - e_4)\\
e_3' := e_3 - e_1'' = e_4 - e_1' =: e_4'\\
e_2' := e_2 - e_3',\ e_2'' := e_1 - e_1' - e_1'' - e_2'
\end{gathered}$$

we can substitute e_1, e_2, e_3, e_4 with

$$\begin{aligned}
e_1' &: \quad n_{110} = n_{011} + \frac{\kappa - \lambda}{2}, \\
e_1'' &: \quad n_{111} = n_{010} + \frac{\kappa - \lambda}{2}, \\
e_2' &: \quad n_{100} = n_{001} + \frac{\kappa + \lambda - n}{2}, \\
e_2'' &: \quad n_{101} = \frac{n + \lambda - \kappa}{2} - n_{011} - n_{010} - n_{001},
\end{aligned}$$

and then e_5, e_6 with

$$\begin{aligned}
n_{010} + n_{011} &= \frac{\mu + \lambda - \kappa}{2}, \\
n_{001} + n_{011} &\neq \frac{n - \kappa}{2}.
\end{aligned}$$

We can easily find a feasible solution of the modified system satisfying also the nonnegativity constraints e_7:

$$\begin{aligned}
0, \frac{\lambda - \kappa}{2} \leq \quad & n_{011} \quad \leq \frac{\mu}{2}, \frac{\mu + \lambda - \kappa}{2}, \\
0, \frac{n - \kappa - \lambda}{2} \leq \quad & n_{001} \quad \leq \frac{n - \mu}{2}, n - 1 - \frac{\kappa + \lambda + \mu}{2}.
\end{aligned}$$

This finishes the proof. □

The counterpart of Theorem 3.2 claims that any three hyperplanes intersect.

THEOREM 3.3. *Let $X, Y \in \mathcal{F}_n$ be arbitrary fixed words. Then,*

$$\mathcal{F}_n = \cup\{Z^\perp : Z \in X^\perp \cap Y^\perp\} \tag{6}$$

holds.

Proof. Assuming $Y = T_1$, we have to show that

$$(\forall W \in \mathcal{F}_n)\ (\exists Z \in T_1^\perp \cap X^\perp)\ WZ \in T_1^\perp. \tag{7}$$

With minor modifications the proof of Theorem 3.2 can be carried through: now we have to find a solution of

$$e_1,\ e_2,\ e_3,\ e_4,\ e_5,\ e_6',\ e_7,$$

where

$$e_6' :\ n_{001} + n_{011} + n_{100} + n_{110} = n/2$$

and $0 \leq \kappa, \lambda, \mu \leq n-2$. Again, eliminating four variables, we are left with the system

$$\begin{aligned} & e'_1,\, e''_1,\, e'_2,\, e''_2, \\ & n_{010} + n_{011} = \frac{\mu + \lambda - \kappa}{2}, \\ & n_{001} + n_{011} = \frac{n - \kappa}{2}, \end{aligned}$$

and, accordingly, with the nonnegativity conditions

$$\begin{array}{rcl} 0, \frac{\lambda - \kappa}{2} \leq & n_{011} & \leq \frac{\mu}{2}, \frac{\mu + \lambda - \kappa}{2}, \\ 0, \frac{n - \kappa - \lambda}{2} \leq & (n-\kappa)/2 - n_{011} & \leq \frac{n - \mu}{2}, n - 1 - \frac{\kappa + \lambda + \mu}{2}. \end{array}$$

Obviously, the solvability of the modified system follows, which concludes the proof. □

Note that the Hadamard conjecture would follow, iteratively, if we could prove Theorem 3.3 for $n-2$ words instead of just two, X, Y. However, we will initiate a more constructive way of proof in the following section.

4 Algorithmical conjecture

In this section we define two types of norms on the space of fixed words, and formulate an algorithmical conjecture, which if true settles the Hadamard conjecture, in general.

Maximal multiplically independent word systems $\mathcal{P} \subseteq \mathcal{F}_n$ (specially, $\mathcal{P} = \mathcal{P}_i$ from $(P2)$) help us to define norms, distances, and scalar products on $\mathcal{F}_n$, as was already mentioned in [8] in the case of the $\mathcal{P}$-norm.

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 $X, Y \in \mathcal{F}_n$ as

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

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

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

Note that $||W||_{\mathcal{P}} = 0$ if and only if $W = T_1$. Furthermore, $W \bullet_{\mathcal{P}} W = ||W||_{\mathcal{P}}^2$.

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) $||X \cdot Y||_{\mathcal{P}} \leq ||X||_{\mathcal{P}} + ||Y||_{\mathcal{P}}$,

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

c) $\varrho_{\mathcal{P}}(X, Y) \leq \varrho_{\mathcal{P}}(X, Z) + \varrho_{\mathcal{P}}(Z, Y)$

hold, for any words $X, Y, Z \in \mathcal{F}_n$. □

Also, applying part b) of Proposition 4.1 for the function $\sqrt{2||.||}$ instead of $||.||$, we obtain readily

COROLLARY 4.1. *With $\mathcal{P} \subseteq \mathcal{F}_n$ as in Proposition 4.1, the inequality*

d) $||X||_{\mathcal{P}} + ||Y||_{\mathcal{P}} - ||X \cdot Y||_{\mathcal{P}} \leq 2\sqrt{||X||_{\mathcal{P}} \cdot ||Y||_{\mathcal{P}}}$

holds, for any words $X, Y \in \mathcal{F}_n$. □

A related notion is motivated by Theorem 2.1. Let us denote by $\nu_{\mathcal{P}}(W)$ the nonnegative integer

$$\nu_{\mathcal{P}}(W) := \left(\frac{n}{2} - ||W||_{\mathcal{P}}\right) \cdot \left(\frac{n}{2} - 1 - ||W||_{\mathcal{P}}\right) \ (W \in \mathcal{F}_n).$$

From Theorem 2.1 it is immediate that

THEOREM 4.1. *Let $\mathcal{P} = \mathcal{P}_i$ denote a subsystem of $\mathcal{R}_n$ with $n-2$ nontrivial elements, as in $(P2)$, and let $W \in \mathcal{F}_n$ be an arbitrary fixed word. Then, $W \in \hat{\mathcal{H}}'_n$ if and only if $\nu_{\mathcal{P}}(W) = 0$.* □

Hence, $\nu_{\mathcal{P}_i}(X \cdot Y)$ on $\mathcal{F}_n$ can be considered as an analogue of the usual scalar product x^*y on $\{\pm 1\}^n$ (in both cases, orthogonality means that the scalar product vanishes).

Moreover, it can easily be verified that (with $\mathcal{P}$ as in Proposition 4.1)

$$\nu_{\mathcal{P}}(X) + \nu_{\mathcal{P}}(Y) \leq \nu_{\mathcal{P}}(X \cdot Y) + \nu_{\mathcal{P}}(T_1), \tag{8}$$

for arbitrary words $X, Y \in \mathcal{F}_n$. This inequality is an analogue of part a) of Proposition 4.1 with the subtle norm instead of the $\mathcal{P}$-norm.

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 *subtle norm* of a word $W \in \mathcal{F}_n$ as

$$|W|_{\mathcal{P}} := \nu_{\mathcal{P}}(T_1) - \nu_{\mathcal{P}}(W).$$

The *subtle scalar product* of two words $X, Y \in \mathcal{F}_n$ will be denoted by

$$X \circ_{\mathcal{P}} Y := \frac{1}{2} \cdot \left(|X|_{\mathcal{P}}^2 + |Y|_{\mathcal{P}}^2 - |X \cdot Y|_{\mathcal{P}}^2\right),$$

also the *subtle distance* of X, Y by

$$\delta_{\mathcal{P}}(X, Y) := |X \cdot Y|_{\mathcal{P}},$$

respectively. Obviously, the relation

$$|W|_{\mathcal{P}} = ||W||_{\mathcal{P}} \cdot (n - 1 - ||W||_{\mathcal{P}}) \ (W \in \mathcal{F}_n)$$

establishes a close relationship between the two types of norms.

Similarly, as in the case of the $\mathcal{P}$-norm, we have

PROPOSITION 4.2. *Let $\mathcal{P} \subseteq \mathcal{F}_n$ be a multiplically independent word system with $n - 2$ elements. Then, the inequalities*

a) $|X \cdot Y|_{\mathcal{P}} \leq |X|_{\mathcal{P}} + |Y|_{\mathcal{P}}$,

b) $\pm(X \circ_{\mathcal{P}} Y) \leq |X|_{\mathcal{P}} \cdot |Y|_{\mathcal{P}}$,

c) $\delta_{\mathcal{P}}(X, Y) \leq \delta_{\mathcal{P}}(X, Z) + \delta_{\mathcal{P}}(Z, Y)$

hold, for any words $X, Y, Z \in \mathcal{F}_n$.

Proof. The inequality in a) follows immediately from (8).

The statement b) can be rewritten as the inequalities

$$\pm(|X|_{\mathcal{P}} - |Y|_{\mathcal{P}}) \leq |X \cdot Y|_{\mathcal{P}} \leq |X|_{\mathcal{P}} + |Y|_{\mathcal{P}},$$

and thus it is equivalent to statement a).

Finally, statement c) is a reformulation of statement a) with the substitution $X \cdot Z$ and $Z \cdot Y$ instead of X and Y, respectively. □

In the case of the analogue of Corollary 4.1, we give a direct proof in order to illustrate the complexity of the statement.

COROLLARY 4.2. *With $\mathcal{P} \subseteq \mathcal{F}_n$ as in Proposition 4.2, the inequality*

d) $|X|_{\mathcal{P}} + |Y|_{\mathcal{P}} - |X \cdot Y|_{\mathcal{P}} \leq 2\sqrt{|X|_{\mathcal{P}} \cdot |Y|_{\mathcal{P}}}$

holds, for any words $X, Y \in \mathcal{F}_n$.

Proof. Let us write the words $X, Y \in \mathcal{F}_n$ as

$$X = \prod_{i \in N_1} P_i \cdot \prod_{j \in N_2} P_j, \ Y = \prod_{j \in N_2} P_j \cdot \prod_{k \in N_3} P_k,$$

where N_1, N_2, N_3 are pairwise disjoint sets of indices with cardinalities n_1, n_2, n_3, respectively. Then,

$$\begin{aligned} \nu_{\mathcal{P}}(T_1) - \nu_{\mathcal{P}}(X) &= (n_1 + n_2) \cdot (n - 1 - n_1 - n_2), \\ \nu_{\mathcal{P}}(T_1) - \nu_{\mathcal{P}}(Y) &= (n_2 + n_3) \cdot (n - 1 - n_2 - n_3); \end{aligned}$$

their product equals $m_{11} \cdot m_{22}$, where

$$\begin{aligned} m_{11} &= n_1 \cdot (n - 1 - n_3) + n_2 \cdot (n - 1 - n_1 - n_2 - n_3), \\ m_{22} &= n_3 \cdot (n - 1 - n_1) + n_2 \cdot (n - 1 - n_1 - n_2 - n_3). \end{aligned}$$

Furthermore,

$$|X|_{\mathcal{P}} + |Y|_{\mathcal{P}} - |X \cdot Y|_{\mathcal{P}} = 2m_{12} = 2m_{21},$$

where

$$m_{12} = m_{21} = n_1 \cdot n_3 + n_2 \cdot (n - 1 - n_1 - n_2 - n_3).$$

Hence, to prove statement d), we have to show the positive semidefiniteness of the (nonnegative) matrix

$$U := \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix}.$$

As the matrix

$$U - n_2 \cdot (n - 1 - n_1 - n_2 - n_3) \cdot J$$

is obviously positive semidefinite, so the positive semidefiniteness of U follows, which finishes the proof. □

We concluded [8] with the paragraph: *We hope that these notions will be useful in the construction and analysis of a Gram–Schmidt-type algorithm (see [4]) 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 Proposition 2.2) *settles the Hadamard conjecture for $n = 4k$, $k = 1, 2, \ldots$.*

Now, we can formulate our guess, the following theoretical algorithm:

ALGORITHM 4.1. We are given a word system

$$W_1, \ldots, W_{n-2} \in T_1^{\perp}$$

(Initially this word system is multiplically independent as in Theorem 2.2.)

Let $W'_1 := W_1$, and let us define iteratively for $1 \leq m < n-2$ the word W'_{m+1} as an optimal solution of the program

$$\min \sum_{i=1}^{m} \nu_{\mathcal{P}_n}(W \cdot W'_i),\ W \in T_1^{\perp}$$

minimizing the distance

$$|W_{m+1} \cdot W'_{m+1}|_{\mathcal{P}_n}.$$

Iterate the above step until the word system

$$W_1 := W'_1, \ldots, W_{n-2} := W'_{n-2}$$

becomes orthogonal.

We mention two examples:

EXAMPLE 4.1. For $n = 8$, with the input multiplically independent word system

$$aac, aad, aca, ada, caa, daa,$$

in one iteration we obtain one of the following orthogonal word systems:

$$aac, ccc, aca, cca, caa, cac$$
$$aac, cdc, cda, ada, caa, cac$$
$$aac, dac, aca, dcc, daa, acc$$
$$aac, dac, aca, dcc, daa, dca,$$

as possible output.

EXAMPLE 4.2. For $n = 8$, with the input multiplically independent word system $\mathcal{B}_{\mathcal{P}_8}$

$$T_2T_3T_4, T_3T_4T_5, T_4T_5T_6, T_5T_6T_7, T_2T_3T_6T_7, T_2T_3T_4T_7$$

in one iteration we obtain the following orthogonal word systems

$$T_2T_3T_4, T_2T_6T_7, T_4T_5T_6, T_3T_5T_7, T_2T_3T_5T_6, T_2T_4T_5T_7,$$
$$T_2T_3T_4, T_2T_6T_7, T_4T_5T_6, T_3T_5T_7, T_2T_3T_5T_6, T_3T_4T_6T_7,$$
$$T_2T_3T_4, T_2T_6T_7, T_4T_5T_6, T_3T_5T_7, T_3T_4T_6T_7, T_2T_4T_5T_7,$$

as three of the possible outputs.

In both examples

$$\sum_{i=1}^{m} \nu_{\mathcal{P}_n}(W'_{m+1} \cdot W'_i) \leq \sum_{i=1}^{m} \nu_{\mathcal{P}_n}(W'_{m+1} \cdot W_i) \leq \sum_{i=1}^{m} \nu_{\mathcal{P}_n}(W_{m+1} \cdot W_i) \qquad (9)$$

holds for $1 \leq m < n - 2$, thus in the course of the algorithm the current word system becomes more and more orthogonal, and also cycling does not occur. Can this proof of the correctness and finiteness of the algorithm be generalized? Is one iteration always enough?

We conjecture that

- the generalization is possible,
- one iteration is not sufficient to reach the desired orthogonal word system, in general,
- local optimization (in 1- or 2-neighbourhoods in the $\mathcal{P}_n$-norm) will prove to be useful in a practical version of the algorithm,

but these lines need further research.

5 Conclusion

In this paper we derived counterparts of algebraical and geometrical results concerning word spaces from previous work of the author. Also, we presented an algorithmical conjecture based on the new results, which if true settles the long-standing Hadamard conjecture on the existence of special orthogonal matrices.

References

1. SZ. V. Jablonszkij and O. B. Lupanov, editors, *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. R. E. A. C. Paley, On orthogonal matrices. *Journal of Mathematics and Physics* 12 (1933), 311-320.

4. G. Strang, *Linear Algebra and its Applications.* Academic Press, New York, 1980.

5. 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.

6. E. Tressler, *A Survey of the Hadamard Conjecture.* M. S. thesis submitted to Virginia Polytechnic Institute and State University, Blacksburg, Virginia, 2004.

7. M. Ujvári, Reformulation of the Hadamard conjecture via Hurwitz-Radon word systems. *Operations Research Reports* No. 2009-02, Department of Operations Research, Eötvös Loránd University of Sciences, Budapest, 2009.

8. M. Ujvári, Multiplically independent word systems. *Operations Research Reports* No. 2011-02, Department of Operations Research, Eötvös Loránd University of Sciences, Budapest, 2011.