Operations Research
Report 2009-02

Reformulation of the Hadamard conjecture via Hurwitz-Radon word systems

Miklós Ujvári

September 2009

Eötvös Loránd University of Sciences
Department of Operations Research

ISSN 1215 - 5918

Reformulation of the Hadamard conjecture via Hurwitz-Radon word systems

Miklós Ujvári

Abstract

The Hadamard conjecture (unsolved since 1867) states that there exists an orthogonal matrix with entries of the same absolute value if and only if the order of the matrix is one, two, or is divisible by four. In the paper we reformulate this conjecture using Hurwitz-Radon word systems. (A Hurwitz-Radon word system is a system of words formed from an alphabet, which is a Klein group, so that the letterwise product of any two different words from the system contains an odd number of the letter b.) We present also algorithms for calculating maximal orthogonal word systems.

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

1 Introduction

One of the conclusions drawn in [9] was that theorems connected with the Lovász number usually have their counterparts. An example of such pair of theorems was Brooks' Theorem and the Alon-Spencer Theorem, or another the Hurwitz-Radon Theorem and (the topic of this paper) the Hadamard conjecture. We start this paper with stating the question which leads us to the Hurwitz-Radon Theorem.

QUESTION 1. *Determine the (m,n) pairs for which there exists a matrix system $R_1,\dots,R_n \in \mathcal{R}^{m\times m}$ such that: a) the matrices R_i are orthogonal, that is $R_i^TR_i = I$, the identity matrix, for all $i = 1,\dots,n$; b) the products $R_i^TR_j$ are skew-symmetric, that is $R_i^TR_j + R_j^TR_i = 0$ for all $i,j = 1,\dots,n$, $i \neq j$.*

Matrix systems with the properties described in Question 1 are called *Hurwitz-Radon matrix system*s. The answer for Question 1 is given by Radon in [6]. Hurwitz studied complex matrix systems in the same context previously, so the following theorem is called the Hurwitz-Radon theorem, see [6], [5], [4]. Here let $\sigma(n)$ denote the number of integers s in the range $0 < s < n$ such that $s \equiv 0,1,2$ or $4 \pmod 8$. For small values of n, the value $\sigma(n)$ can be read out from the following table:

n	1	2	3,4	5,6,7,8
$\sigma(n)$	0	1	2	3
n	9	10	11,12	13,14,15,16
$\sigma(n)$	4	5	6	7

The table can be continued in a similar manner for larger values of n.

THEOREM 1.1. (Hurwitz-Radon) *There exists a Hurwitz-Radon matrix system $R_1,\dots,R_n \in \mathcal{R}^{m\times m}$ if and only if $m \equiv 0 \pmod{2^{\sigma(n)}}$.*

As a counterpart of Question 1 the following question arises in [9].

QUESTION 2. *Determine the (m,n) pairs for which there exists a matrix system $H_1,\dots,H_n \in \mathcal{R}^{m\times m}$ such that: a) the matrices H_i are orthogonal, that is $H_i^TH_i = I$ for all $i = 1,\dots,n$; b) the products $H_i^TH_j$ are symmetric and have zero trace, that is $H_i^TH_j = H_j^TH_i$ and $\operatorname{tr}(H_i^TH_j) = 0$ for all $i,j = 1,\dots,n$, $i \neq j$.*

We can suppose that $H_1 = I$, then using simultaneous diagonalization [5] that the matrices $H_1,\dots,H_n$ are diagonal. This way we reformulated Question 2 as Question 3 below.

QUESTION 3. *Determine the (m,n) pairs for which there exists a so-called* Hadamard matrix $H \in \{\pm 1\}^{m\times n}$ *such that $H^TH = mI$.*

CONJECTURE: *The (m,n) pairs satisfying the requirements of either Question 2 or Question 3 are:*

- *$(m,1)$ such that $m \geq 1$;*
- *$(m,2)$ such that $m \geq 2$ is even;*
- *(m,n) such that $m \geq n$ and $m \equiv 0 \pmod 4$.*

Necessity can be easily verified, see [7]. The remaining nontrivial part of the conjecture is stated as the

HADAMARD CONJECTURE: *A square Hadamard matrix* $H \in \{\pm 1\}^{m\times m}$ *exists if* $m \equiv 0 \pmod 4$.

It is interesting to note that it was Sylvester who first studied Hadamard matrices in 1867. In spite of this fact they are called Hadamard matrices because of their connection with the determinantal Hadamard theorem. This theorem (see [1], Exercise 7.d.8) states that the absolute value of the determinant of a square real matrix is at most the product of the euclidean norms of the column vectors of the matrix. If $H \in \{\pm 1\}^{m\times m}$ is an Hadamard matrix with column vectors $h_1, \ldots, h_m \in \{\pm 1\}^m$ then equality holds: $\det H = ||h_1|| \cdot \ldots \cdot ||h_m||$. On the other hand, if for a matrix $H \in \{\pm 1\}^{m\times m}$ the equality $\det H = ||h_1|| \cdot \ldots \cdot ||h_m||$ holds then the column vectors are necessarily pairwise orthogonal ([1]), thus H is an Hadamard matrix ([7]).

The Hadamard conjecture presently is verified for all $m < 668$ ([3]). For a historical overview we refer to [8], [2].

The main idea in this paper is that we can search for orthogonal ± 1-vectors among vectors related with image vectors of Hurwitz-Radon word systems, where orthogonality of the ± 1-vectors can be checked by verifying that the product of the corresponding words is in a specified word set. In Section 2 the definition of Hurwitz-Radon word systems is described. In Section 3 the image vectors of a Hurwitz-Radon word system are characterized. In Section 4 we present a formula connecting multiplication of words and addition of image vectors. The main result of the paper (a reformulation of the Hadamard conjecture) is derived in Section 5. Here also two algorithms are presented, for calculating maximal orthogonal word systems.

2 Hurwitz-Radon word systems

In this section Hurwitz-Radon word systems are defined. Their connection with Hurwitz-Radon matrix systems makes possible the determination of a Hurwitz-Radon word system with maximum number of elements.

Let us suppose that we are given an alphabet $\mathcal{A}$ of the letters a, b, c, and d which form 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

Then we can multiply two words W_1, W_2 made up of the same number s of letters of the alphabet: the result will be 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 $(1 \le i \le s)$. For example, in the case $W_1 = abc$, $W_2 = ccd$ the product is $W_1 \cdot W_2 = cdb$.

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 $(i \neq j)$ from the system.

For example, in the case $s = 2$ a word system $W_1, \ldots, W_n \in \mathcal{A}^2$ is a Hurwitz-Radon word system if and only if its words are the elements of either the same row or the same column of the following table:

aa	cb	ba	db
ab	ca	bb	da
bc	dd	ac	cd
bd	dc	ad	cc

In this case maximal Hurwitz-Radon word systems (which are not contained in another Hurwitz-Radon word system as a proper subsystem) are also the ones with the largest number of elements. This statement does not hold generally: in the case $s = 8$ it can be easily verified that the Hurwitz-Radon word system aaa, acb, aba, adb is maximal, and has less element than the Hurwitz-Radon word system $aaa, ccb, cba, cdb, baa, dab, dbc, dbd$.

Given a Hurwitz-Radon word system we can easily define a corresponding Hurwitz-Radon matrix system. The letters of the alphabet a, b, c, and d correspond to the matrices

$$A := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, B := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, C := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, D := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

respectively. Words correspond to the Kronecker product of the matrices corresponding to their letters: for example the word dbc corresponds to the matrix $D \otimes B \otimes C$ where $\otimes$ denotes Kronecker product. (For the definition of the Kronecker product, see [5].) It can be easily seen ([9]) that then Hurwitz-Radon word systems correspond to Hurwitz-Radon matrix systems.

This construction and the Hurwitz-Radon theorem gives that the maximum number n of words in a Hurwitz-Radon word system $W_1, \ldots, W_n \in \mathcal{A}^s$ is at most $\max\{n : s \ge \sigma(n)\}$. (Really, if there exists a Hurwitz-Radon word system of s-letter words $W_1, \ldots, W_n$, then by the above construction there exists a Hurwitz-Radon matrix system of $2^s \times 2^s$ matrices $R_1, \ldots, R_n$. By the Hurwitz-Radon theorem this is equivalent to the equation $2^s \equiv 0 \pmod{2^{\sigma(n)}}$, that is $\sigma(n) \le s$.)

We will show that the bound $\max\{n : s \geq \sigma(n)\}$ can be realized. This statement is the immediate consequence of the following lemma from [9] which we restate here with proof for completeness.

LEMMA 2.1. *If $n \geq 2$ then there exists a Hurwitz-Radon word system $W_1, \ldots, W_n \in \mathcal{A}^{\sigma(n)}$.*

Proof. For the values $2 \leq n \leq 9$ the following word-sets have the desired property:

$$\begin{array}{rl} n = 2,\ \sigma(n) = 1: & a, b \\ n = 3 \text{ or } 4,\ \sigma(n) = 2: & \text{any } n \text{ words from the word-set } aa, cb, ba, db \\ n = 5, 6, 7 \text{ or } 8,\ \sigma(n) = 3: & \text{any } n \text{ words from the word-set} \\ & aaa, ccb, cba, cdb, baa, dab, dbc, dbd \\ n = 9,\ \sigma(n) = 4: & aaaa, accb, acba, acdb, abaa \\ & adab, adbc, cdbd, ddbd. \end{array}$$

For larger values of n we can use the following induction argument. Let us denote by $S_1, \ldots, S_9$ the words defined above in the case $n = 9$. Suppose that for some n we have appropriate $\sigma(n)$-letter words $T_1, \ldots, T_n$. Then the word-set

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

where & denotes concatenation, is made up of $n+8$ of $(\sigma(n)+4)$-letter words, and also has the desired property. Thus the statement in the lemma is dealt with for all the values of n. □

Summarizing, we have

THEOREM 2.1. *The maximum number n of words in a Hurwitz-Radon word system $W_1, \ldots, W_n \in \mathcal{A}^s$ equals* $\max\{n : s \geq \sigma(n)\}$. □

Because of their importance in what follows, the Hurwitz-Radon word systems constructed in the proof of Lemma 2.1 will be denoted by $\mathcal{R}_n$ for all $n \equiv 1, 2, 4, \text{ or } 0 \pmod 8$.

3 Images of words

In this section we will characterize the image vectors of the word systems $\mathcal{R}_n$ defined in the previous section.

So far we considered word systems as ordered sets of words written horizontally, consecutively. Now, a word system $R_1, \ldots, R_n \in \mathcal{A}^s$ can be considered

as a matrix from $\mathcal{A}^{n\times s}$ whose rows are formed by the words $R_1, \ldots, R_n$. 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 $\mathcal{R}$. A *column system of words* can be defined similarly. We denote by $[\mathcal{C}]$ that the word system $\mathcal{C}$ is considered as a column system. The corresponding matrix of letters is denoted similarly.

Given two words $W_1 \in \mathcal{A}^{1\times s}$ and $[W_2] \in \mathcal{A}^{s\times 1}$, their *symmetricity product* $W_1[W_2]$ is defined as the total number of the letter bs in the word $W_1 \cdot W_2$ taken modulo 2. For example, $ab[cc] = 0$ and $cd[da] = 1$. (Note that with the corresponding matrices – see Section 2 – the matrix $(A \otimes B) \cdot (C \otimes C)$ is symmetric, while the matrix $(C \otimes D) \cdot (D \otimes A)$ is skew-symmetric, which accounts for the name of the symmetricity product.)

For two word systems $\mathcal{R} = (R_1, \ldots, R_n) \in \mathcal{A}^{n\times s}$ and $\mathcal{C} = (C_1, \ldots, C_m) \in \mathcal{A}^{m\times s}$, their *symmetricity product* is the matrix $\mathcal{R}[\mathcal{C}] \in \{0,1\}^{n\times m}$ whose (i,j)-th element is $R_i[C_j]$ for all $1 \leq i \leq n$, $1 \leq j \leq m$. For example,

$$ab, cd[cc, da] = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

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

Let us denote by $\operatorname{Im}\mathcal{R}_n$ the set of so called *image vector*s $v \in \{0,1\}^n$ for which there exists a word $W \in \mathcal{A}^{\sigma(n)}$ such that $v = \mathcal{R}_n[W]$, where $n \equiv 1, 2, 4, \text{ or } 0 \pmod 8$. Next, in this section we will characterize the set $\operatorname{Im}\mathcal{R}_n$ for all $n \equiv 0 \pmod 4$.

The following lemma can be verified by a simple computer program. Here $\mathbf{1}$ denotes the vector with all elements equal to one.

LEMMA 3.1. *It holds that*

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

For $n = 8, 9$, the mapping $W \mapsto \mathcal{R}_n[W]$ is a bijection between the sets $\mathcal{A}^{\sigma(n)}$ and $\operatorname{Im}\mathcal{R}_n$. 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.

Proof. The case $n = 4$ can be dealt with by listing the vectors of $\operatorname{Im}\mathcal{R}_4$. In the cases $n = 8, 9$ to verify the equation (1) it is enough to check the inclusion

$$\operatorname{Im}\mathcal{R}_n \subseteq \left\{ v \in \{0,1\}^n \,\middle|\, \mathbf{1}^T v = \begin{cases} 3 \text{ or } 7, & \text{if } n = 8, \\ 0, 3, 4, 7, \text{ or } 8, & \text{if } n = 9 \end{cases} \right\}$$

and the injectivity of the mapping $W \mapsto \mathcal{R}_n[W]$. Really, the set $\mathcal{A}^{\sigma(n)}$ and the set on the right hand side of (1) have the same cardinality, thus necessarily the equation (1) holds (and the mapping $W \mapsto \mathcal{R}_n[W]$ is superjective also). To prove the last statement of the lemma, verify that for the vectors $v \in \mathrm{Im}\,(\mathcal{R}_9 \cup (bdbd))$, the equation $\mathbf{1}^T v = 0, 4$, or 8 holds. □

Now, the main results of the section follow.

THEOREM 3.1. *It holds that*

$$\mathrm{Im}\,\mathcal{R}_n = \left\{v \in \{0,1\}^n : \mathbf{1}^T v \equiv 1 \pmod 2\right\},$$

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

Proof. First, we will prove that for $n \equiv 4 \pmod 8$,

$$\mathrm{Im}\,\mathcal{R}_n \subseteq \left\{v \in \{0,1\}^n : \mathbf{1}^T v \equiv 1 \pmod 2\right\}. \tag{2}$$

The proof is by induction on n. By Lemma 3.1 the statement holds for $n = 4$. Let us suppose that it holds for n, and let us prove it for $n+8$. Let us denote by $S_1, \ldots, S_9$ and $T_1, \ldots, T_n$ the same words as in the proof of Lemma 2.1, and let $S_{10} := bdbd$. Let us choose a vector v from $\mathrm{Im}\,\mathcal{R}_{n+8}$, then v is of the form $v = (v_1, \ldots, v_{n+8})$, where

$$\begin{aligned} v_i &= (S_i \& T_1)[X \& Y] = S_i[X] + T_1[Y] \bmod 2 \ (1 \le i \le 9) \\ v_{j+8} &= (S_{10} \& T_j)[X \& Y] = S_{10}[X] + T_j[Y] \bmod 2 \ (2 \le j \le n) \end{aligned}$$

for some vectors $X \in \mathcal{A}^4$, $Y \in \mathcal{A}^{\sigma(n)}$. Let us denote by Σ_1 and Σ_2 the sums of the elements $v_1, \ldots, v_9$ and $v_{10}, \ldots, v_{n+8}$, respectively. We have to show that $\Sigma_1 + \Sigma_2 \equiv 1 \pmod 2$.

Note that $0 \le \Sigma_1 \le 9$. It can be easily seen that

$$\Sigma_1 = 0 \iff T_1[Y] = 0 \text{ and } \sum_{i=1}^{9} S_i[X] = 0.$$

There are nine similar statements depending on the value of Σ_1, their datas can be read out from the following table:

Σ_1	1	2	3	4	5	6	7	8	9
$T_1[Y]$	1	1	0	0	1	1	0	0	1
$\sum_{i=1}^{9} S_i[X]$	8	7	3	4	4	3	7	8	0

We have to deal with two cases

- Case 1: $\Sigma_1 = 0, 1, 4, 5, 8$, or 9;
- Case 2: $\Sigma_1 = 2, 3, 6$, or 7.

In Case 1, by Lemma 3.1, $S_{10}[X] = 0$. Hence, $v_{j+8} = T_j[Y]$ $(2 \le j \le n)$, and we have

$$\Sigma_1 + \Sigma_2 = \Sigma_1 - T_1[Y] + \sum_{j=1}^{n} T_j[Y],$$

an odd number, as by induction the sum $\sum_{j=1}^{n} T_j[Y]$ is odd. In Case 2, by Lemma 3.1, $S_{10}[X] = 1$. Hence, $v_{j+8} = 1 - T_j[Y]$ $(2 \le j \le n)$, and we have

$$\Sigma_1 + \Sigma_2 = \Sigma_1 + T_1[Y] - 1 + n - \sum_{j=1}^{n} T_j[Y],$$

an odd number, as by induction the sum $n - \sum_{j=1}^{n} T_j[Y]$ is odd. This way in all the two cases we verified the inclusion (2).

To prove the reverse inclusion we again use induction on n. The statement is true for $n = 4$ by Lemma 3.1. Let us suppose that it holds for n and let us prove it for $n + 8$. Thus we are given a vector of the form $v = (v_1, \ldots, v_{n+8})$ such that for the sums of the elements $v_1, \ldots, v_9$ and $v_{10}, \ldots, v_{n+8}$ (denoted by Σ_1 and Σ_2, respectively) the equation $\Sigma_1 + \Sigma_2 \equiv 1 \pmod 2$ holds. We have to show that $v = \mathcal{R}_{n+8}[X \& Y]$ for some words $X \in \mathcal{A}^4$, $Y \in \mathcal{A}^{\sigma(n)}$. This statement can be proved simply by repeating the previous part of the proof with the necessary modifications, and therefore is omitted. □

The following theorem can be proved similarly as Theorem 3.1.

THEOREM 3.2. *It holds that*

$$\mathrm{Im}\,\mathcal{R}_n = \left\{v \in \{0,1\}^n : \mathbf{1}^T v \equiv 3 \pmod 4\right\},$$

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* $\mathrm{Im}\,\mathcal{R}_n$. □

4 Images of products

In this section we derive a theorem describing a connection between the multiplicative structure of the words and the additive structure of the image vectors.

Given two vectors $v, w \in \{0,1\}^n$ we denote by $v +_2 w$ their sum modulo 2, that is $v +_2 w$ is the n-vector with i-th element $(v +_2 w)_i = (v)_i + (w)_i \bmod 2$ $(1 \le i \le n)$.

If for the vectors $v, w \in \{0,1\}^n$ the equations $\mathbf{1}^T v \equiv 1 \equiv \mathbf{1}^T w \pmod 2$ hold, as in the case of the image vectors $\mathcal{R}_n[W]$, $W \in \mathcal{A}^{\sigma(n)}$, then necessarily $\mathbf{1}^T(v +_2 w) \equiv 0 \pmod 2$. Thus, in order to remain in the set of the image vectors, we have to make a "flaw" in the definition of $v +_2 w$: for the vectors $v, w \in \{0,1\}^n$ we will denote by $v \oplus_2 w$ the n-vector whose i-th element is

$$(v \oplus_2 w)_i = \begin{cases} 1 - (v +_2 w)_i, & \text{if } i = 1, \\ (v +_2 w)_i, & \text{if } 2 \le i \le n. \end{cases}$$

The negation of the vector $v \in \{0,1\}^n$ will be denoted by $\overline{v}$. Thus $\overline{v}$ is the n-vector with i-th element $(\overline{v})_i = 1 - (v)_i$ $(1 \le i \le n)$. It can be easily verified that the equations

$$\overline{v} \oplus_2 w = \overline{v \oplus_2 w} = v \oplus_2 \overline{w},\ \overline{v} \oplus_2 \overline{w} = v \oplus_2 w$$

hold, for every $v, w \in \{0,1\}^n$.

The main result of the section is the following formula connecting the multiplication of the words and the addition of the image vectors:

$$\mathcal{R}_n[W_1 \cdot W_2] = \begin{cases} \mathcal{R}_n[W_1] \oplus_2 \mathcal{R}_n[W_2] \\ \text{or} \\ \overline{\mathcal{R}_n[W_1] \oplus_2 \mathcal{R}_n[W_2]} \end{cases} \tag{3}$$

for every pair of words $W_1, W_2 \in \mathcal{A}^{\sigma(n)}$, and for all $n \equiv 1, 2, 4$, or $0 \pmod 8$. Note that examining the first element of the vectors $\mathcal{R}_n[W_1 \cdot W_2]$ and $\mathcal{R}_n[W_1] \oplus_2 \mathcal{R}_n[W_2]$, we can decide whether these vectors are equal or the negation of each other.

To prove the formula (3) generally, we will need the special cases $n = 2, 4, 8$, and 9. The following lemma can be verified by a simple computer program.

LEMMA 4.1. *Formula (3) holds in the cases $n = 2, 4, 8$, and 9. Furthermore, in the case $n = 9$ the equation $\mathcal{R}_n[W_1 \cdot W_2] = \mathcal{R}_n[W_1] \oplus_2 \mathcal{R}_n[W_2]$ implies the equation*

$$bdbd[W_1 \cdot W_2] = \overline{bdbd[W_1] +_2 bdbd[W_2]},$$

and the equation $\mathcal{R}_n[W_1 \cdot W_2] = \overline{\mathcal{R}_n[W_1] \oplus_2 \mathcal{R}_n[W_2]}$ implies the equation

$$bdbd[W_1 \cdot W_2] = bdbd[W_1] +_2 bdbd[W_2],$$

for all words $W_1, W_2 \in \mathcal{A}^4$.

Proof. The statement follows by checking the validity of formula (3) for the word systems $\mathcal{R}_2$, $\mathcal{R}_4$, $\mathcal{R}_8$, and $\mathcal{R}_9 \cup (adbd)$. □

Now, the general case follows.

THEOREM 4.1. *Formula (3) holds for all $n \equiv 1, 2, 4$, and $0 \pmod 8$.*

Proof. The proof is by induction. By Lemma 4.1 the statement holds for $n = 2, 4, 8, 9$. We suppose that formula (3) holds for n and we will prove that it holds for $n + 8$.

Let us denote by $S_1, \ldots, S_9$ and $T_1, \ldots, T_n$ the same words as in the proof of Lemma 2.1. Moreover, let us denote by S_{10} the word $bdbd$, and let us denote by $\mathcal{R}'_n$ the word system made up of the words $T_2, \ldots, T_n$.

We have to show that for the vectors

$$\begin{aligned} v_1 &:= \mathcal{R}_9[X_1 \cdot X_2] +_2 T_1[Y_1 \cdot Y_2]\mathbf{1}, \\ w_1 &:= (\mathcal{R}_9[X_1] +_2 T_1[Y_1]\mathbf{1}) \oplus_2 (\mathcal{R}_9[X_2] +_2 T_1[Y_2]\mathbf{1}), \\ v_2 &:= S_{10}[X_1 \cdot X_2]\mathbf{1} +_2 \mathcal{R}'_n[Y_1 \cdot Y_2], \\ w_2 &:= (S_{10}[X_1]\mathbf{1} +_2 \mathcal{R}'_n[Y_1]) +_2 (S_{10}[X_2]\mathbf{1} +_2 \mathcal{R}'_n[Y_2]) \end{aligned}$$

either $v_1 = w_1$ and $v_2 = w_2$, or $v_1 = \overline{w_1}$ and $v_2 = \overline{w_2}$, where $X_1, X_2 \in \mathcal{A}^4$, $Y_1, Y_2 \in \mathcal{A}^{\sigma(n)}$. (In other words, that formula (3) holds for $n + 8$ with the words $W_1 = X_1 \& Y_1$, $W_2 = X_2 \& Y_2$.)

We have to deal with four cases:

- Case 1: $T_1[Y_1] = T_1[Y_2]$ and $T_1[Y_1 \cdot Y_2] = 0$;
- Case 2: $T_1[Y_1] = T_1[Y_2]$ and $T_1[Y_1 \cdot Y_2] = 1$;
- Case 3: $T_1[Y_1] \ne T_1[Y_2]$ and $T_1[Y_1 \cdot Y_2] = 0$;
- Case 4: $T_1[Y_1] \ne T_1[Y_2]$ and $T_1[Y_1 \cdot Y_2] = 1$.

Let us first consider the case when $T_1[Y_1] = T_1[Y_2]$ and $T_1[Y_1 \cdot Y_2] = 0$. Then $T_1[Y_1] \oplus_2 T_1[Y_2] = 1$ and $T_1[Y_1 \cdot Y_2] = 0$, necessarily by formula (3) for n, we have

$$\mathcal{R}_n[Y_1 \cdot Y_2] = \overline{\mathcal{R}_n[Y_1] \oplus_2 \mathcal{R}_n[Y_2]}. \tag{4}$$

Furthermore,

$$v_1 = \mathcal{R}_9[X_1 \cdot X_2],\ w_1 = \mathcal{R}_9[X_1] \oplus_2 \mathcal{R}_9[X_2]$$

using the equation $\overline{v} \oplus_2 \overline{w} = v \oplus_2 w$, $v, w \in \{0,1\}^9$.

By Lemma 4.1 either the equation

$$\mathcal{R}_9[X_1 \cdot X_2] = \mathcal{R}_9[X_1] \oplus_2 \mathcal{R}_9[X_2], \tag{5}$$

or the equation

$$\mathcal{R}_9[X_1 \cdot X_2] = \overline{\mathcal{R}_9[X_1] \oplus_2 \mathcal{R}_9[X_2]} \tag{6}$$

holds.

Let us suppose first that formula (5) holds. Then $v_1 = w_1$, and by Lemma 4.1,

$$S_{10}[X_1 \cdot X_2] = \overline{S_{10}[X_1] +_2 S_{10}[X_2]}.$$

Consequently, by (4) $v_2 = w_2$, and the statement follows as $v_1 = w_1$ and $v_2 = w_2$.

Let us suppose now that formula (6) holds. Then $v_1 = \overline{w_1}$, and by Lemma 4.1,

$$S_{10}[X_1 \cdot X_2] = S_{10}[X_1] +_2 S_{10}[X_2].$$

Consequently, by (4) $v_2 = \overline{w_2}$, and the statement follows as $v_1 = \overline{w_1}$ and $v_2 = \overline{w_2}$.

The cases 2, 3, and 4 can be dealt with similarly. Hence, the theorem is proved. □

5 Reformulation and algorithms

In this section we reformulate the Hadamard conjecture using a characterization of the orthogonality of words. Also two algorithms are presented for calculating maximal orthogonal word systems.

The following lemmas will be needed.

LEMMA 5.1. *For the vectors $v, w \in \{0,1\}^n$ the following statements are equivalent:*

a) the vectors $2v - \mathbf{1}$ and $2w - \mathbf{1}$ are orthogonal;

b) $\mathbf{1}^T(v +_2 w) = n/2$*;*

c) $\mathbf{1}^T(v \oplus_2 w) = \begin{cases} n/2-1, & \text{if } (v \oplus_2 w)_1 = 0, \\ n/2+1, & \text{if } (v \oplus_2 w)_1 = 1; \end{cases}$

d) $\mathbf{1}^T(\overline{v \oplus_2 w}) = \begin{cases} n/2-1, & \text{if } (\overline{v \oplus_2 w})_1 = 0, \\ n/2+1, & \text{if } (\overline{v \oplus_2 w})_1 = 1. \end{cases}$

Proof. The equivalences *a)* $\Longleftrightarrow$ *b)*, *b)* $\Longleftrightarrow$ *c)* are straightforward. To prove the equivalence *a)* $\Longleftrightarrow$ *d)* note that statement a) is equivalent to statement a) for the vectors $v, \overline{w}$, and that statement d) is equivalent to statement c) for the vectors $v, \overline{w}$. □

Two words $W_1, W_2 \in \mathcal{A}^{\sigma(n)}$ are called *orthogonal*, if the vectors $2\mathcal{R}_n[W_1] - \mathbf{1}$ and $2\mathcal{R}_n[W_2] - \mathbf{1}$ are orthogonal.

LEMMA 5.2. *The words $W_1, W_2 \in \mathcal{A}^{\sigma(n)}$ are orthogonal if and only if $W_1 \cdot W_2 \in \hat{\mathcal{H}}_n$, where the word set $\hat{\mathcal{H}}_n$ is defined as:*

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

Proof. Necessity: Let us suppose that the words W_1 and W_2 are orthogonal. Then by part c) and d) of Lemma 5.1 we have:

- $\mathbf{1}^T(\mathcal{R}_n[W_1] \oplus_2 \mathcal{R}_n[W_2]) = \begin{cases} n/2-1, & \text{if } (\mathcal{R}_n[W_1])_1 \neq (\mathcal{R}_n[W_2])_1, \\ n/2+1, & \text{if } (\mathcal{R}_n[W_1])_1 = (\mathcal{R}_n[W_2])_1. \end{cases}$
- $\mathbf{1}^T(\overline{\mathcal{R}_n[W_1] \oplus_2 \mathcal{R}_n[W_2]}) = \begin{cases} n/2-1, & \text{if } (\mathcal{R}_n[W_1])_1 = (\mathcal{R}_n[W_2])_1, \\ n/2+1, & \text{if } (\mathcal{R}_n[W_1])_1 \neq (\mathcal{R}_n[W_2])_1. \end{cases}$

We have to deal with four cases:

- Case 1: $(\mathcal{R}_n[W_1])_1 = (\mathcal{R}_n[W_2])_1$ and $(\mathcal{R}_n[W_1 \cdot W_2])_1 = 0$;
- Case 2: $(\mathcal{R}_n[W_1])_1 = (\mathcal{R}_n[W_2])_1$ and $(\mathcal{R}_n[W_1 \cdot W_2])_1 = 1$;
- Case 3: $(\mathcal{R}_n[W_1])_1 \neq (\mathcal{R}_n[W_2])_1$ and $(\mathcal{R}_n[W_1 \cdot W_2])_1 = 0$;
- Case 4: $(\mathcal{R}_n[W_1])_1 \neq (\mathcal{R}_n[W_2])_1$ and $(\mathcal{R}_n[W_1 \cdot W_2])_1 = 1$;

Let us consider first Case 1. In this case by Theorem 4.1 the equation

$$\mathcal{R}_n[W_1 \cdot W_2] = \overline{\mathcal{R}_n[W_1] \oplus_2 \mathcal{R}_n[W_2]}$$

holds. Hence,

$$\mathbf{1}^T(\mathcal{R}_n[W_1 \cdot W_2]) = \mathbf{1}^T(\overline{\mathcal{R}_n[W_1] \oplus_2 \mathcal{R}_n[W_2]}) = n/2 - 1,$$

as $(\mathcal{R}_n[W_1])_1 = (\mathcal{R}_n[W_2])_1$, and this was to be shown, as $(\mathcal{R}_n[W_1 \cdot W_2])_1 = 0$.

The cases 2, 3, and 4 can be dealt with similarly, thus the "only if" part of the lemma is proved.

Sufficiency: Let us suppose now, that the equation

$$\mathbf{1}^T(\mathcal{R}_n[W_1 \cdot W_2]) = \begin{cases} n/2-1, & \text{if } (\mathcal{R}_n[W_1 \cdot W_2])_1 = 0, \\ n/2+1, & \text{if } (\mathcal{R}_n[W_1 \cdot W_2])_1 = 1 \end{cases}$$

holds. By Theorem 4.1 we have two cases:

$$\mathcal{R}_n[W_1 \cdot W_2] = \begin{cases} \mathcal{R}_n[W_1] \oplus_2 \mathcal{R}_n[W_2] \\ \text{or} \\ \overline{\mathcal{R}_n[W_1] \oplus_2 \mathcal{R}_n[W_2]}. \end{cases}$$

Orthogonality of the words W_1 and W_2 follows from part c) of Lemma 5.1 in the first case, and from part d) of Lemma 5.1 in the second case. Hence, the "if" part of the lemma is proved as well. □

Now, we can reformulate the Hadamard conjecture as

CONJECTURE 5.1. *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 5.1. *The Hadamard conjecture and Conjecture 5.1 are equivalent.*

Proof. First, if $\mathcal{H} = (H_2, \ldots, H_n)$ is a word system with the properties described in Conjecture 5.1, then by Lemma 5.2 the vectors

$$h_1 := 2\mathcal{R}_n[a \ldots a] - \mathbf{1}, h_2 := 2\mathcal{R}_n[H_2] - \mathbf{1}, \ldots, h_n := 2\mathcal{R}_n[H_n] - \mathbf{1}$$

as column vectors form an Hadamard matrix $H \in \{\pm 1\}^{n \times n}$.

On the other hand, let us suppose that $H \in \{\pm 1\}^{n \times n}$ is an Hadamard matrix with column vectors $h_1, \ldots, h_n \in \{\pm 1\}^n$. Then there exist vectors $v_1, \ldots, v_n \in \{0,1\}^n$ such that $h_i = 2v_i - \mathbf{1}$ for $1 \le i \le n$. Multiplying the row vectors of the matrix H by -1 if necessary, we can suppose that $v_1 = \mathcal{R}_n[a \ldots a]$.

Then $v_1 \oplus_2 v_i = \overline{v_i}$ for $i = 2, \ldots, n$. Moreover, the orthogonality of the vectors h_1 and h_i $(2 \le i \le n)$ by Lemma 5.1 implies

$$\mathbf{1}^T \overline{v_i} = \mathbf{1}^T(v_1 \oplus_2 v_i) = n/2 - 1 \text{ or } n/2 + 1 \ (2 \le i \le n).$$

Hence, we have

$$\mathbf{1}^T v_i \equiv -1 \text{ or } \mathbf{1}^T \overline{v_i} \equiv -1 \pmod{2 \text{ and } 4}.$$

By Theorems 3.1 and 3.2, respectively, there exists a word set $H_2, \ldots, H_n \subseteq \mathcal{A}^{\sigma(n)}$ such that

$$v_i = \mathcal{R}_n[H_i] \text{ or } \overline{v_i} = \mathcal{R}_n[H_i] \ (2 \le i \le n).$$

It can be easily verified using Lemma 5.2 that then the word set $\mathcal{H}$ made up of the words $H_2, \ldots, H_n$ meets the requirements of Conjecture 5.1. □

Based on Lemma 5.2 the following two algorithms can be easily analyzed, and Theorem 5.2 can be derived on the properties of their output.

ALGORITHM 1.

- *Initially, let $W_1 \in \hat{\mathcal{H}}_n$, and let $\mathcal{H}_1 := (W_1)$.*
- *In the k-th step we are given a word set $W_1, \ldots, W_k$ such that*

  $$\mathcal{H}_k := (W_1, \ldots, W_k) \subseteq \hat{\mathcal{H}}_n.$$

  Let us choose a word W_{k+1} such that

  $$W_{k+1} \in \hat{\mathcal{H}}_n, W_{k+1} \cdot W \in \hat{\mathcal{H}}_n \ (W \in \mathcal{H}_k).$$

- *Terminate if there exists no such a word W_{k+1}. Otherwise continue with the $(k+1)$-th step.*

ALGORITHM 2.

- *Initially, let $W_1 \in \hat{\mathcal{H}}_n$, and let $\mathcal{H}'_1 := (W_1)$.*
- *In the k-th step we are given a word set $W_1, \ldots, W_k$ such that*

  $$\mathcal{H}'_k := (W_1^{\varepsilon_1} \cdot \ldots \cdot W_k^{\varepsilon_k} : \varepsilon_1, \ldots, \varepsilon_k = 0 \text{ or } 1, \varepsilon_1 + \ldots + \varepsilon_k > 0) \subseteq \hat{\mathcal{H}}_n,$$

  where $W^0 := a \ldots a$. Let us choose a word W_{k+1} such that

  $$W_{k+1} \in \hat{\mathcal{H}}_n, W_{k+1} \cdot W \in \hat{\mathcal{H}}_n \ (W \in \mathcal{H}'_k).$$

- *Terminate if there exists no such a word W_{k+1}. Otherwise continue with the $(k+1)$-th step.*

Note that during the algorithms the inclusions

$$\mathcal{H}_k \subseteq \hat{\mathcal{H}}_n,\ \mathcal{H}_k \cdot \mathcal{H}_k \subseteq \hat{\mathcal{H}}_n,\ \mathcal{H}'_k \cdot \mathcal{H}'_k \subseteq \mathcal{H}'_k \subseteq \hat{\mathcal{H}}_n$$

remain true, where $\mathcal{H} \cdot \mathcal{H}$ denotes the words of the form $W_1 \cdot W_2$ ($W_1, W_2 \in \mathcal{H}$, $W_1 \neq W_2$). From this observation easily follows

THEOREM 5.2. *Algorithm 1 determines a maximal (as regards inclusion) word system $\mathcal{H}$ such that $\mathcal{H} \subseteq \hat{\mathcal{H}}_n$ and $\mathcal{H} \cdot \mathcal{H} \subseteq \hat{\mathcal{H}}_n$. Algorithm 2 determines a maximal word system $\mathcal{H}'$ such that $\mathcal{H}' \subseteq \hat{\mathcal{H}}_n$ and $\mathcal{H}' \cdot \mathcal{H}' \subseteq \mathcal{H}'$.* □

The advantage of Algorithm 2 over Algorithm 1 is that in the case of Algorithm 2 in order to find an output word system with $n-1$ elements we have to check orthogonality only $O(n)$ times in the optimal case, while in the case of Algorithm 1 this number is $O(n^2)$. However generally, for all $n \equiv 0 \pmod 4$, the Algorithm 2 can not find a square Hadamard matrix. In fact, $\mathcal{H}' \cup \{a\}^{\sigma(n)}$ is a subgroup of the group $\mathcal{A}^{\sigma(n)}$, thus the order of $\mathcal{H}'$ plus one is a divisor of the order of $\mathcal{A}^{\sigma(n)}$, that is $4^{\sigma(n)}$. Necessarily the order of $\mathcal{H}'$ is of the form $2^s - 1$.

CONJECTURE 5.2. *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 $\max\{2^s - 1 : 2^s \leq n\}$; 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 $\mathcal{H}'$, too.*

(Note that for $n = 4, 8$ the word system $\mathcal{H}' := \{a, d\}^{\sigma(n)} \setminus \{a\}^{\sigma(n)}$ meets the requirements of Conjecture 5.2.)

Conclusion. In this paper we described a reformulation of the Hadamard conjecture. Instead of orthogonality of vectors we studied orthogonality of words. Orthogonality of words was defined via Hurwitz-Radon word systems, and can be checked by verifying that the product of the words is in a specified word set. Based on this fact, we analyzed two algorithms for calculating maximal orthogonal word sets.

References

1. Á. Császár, *Real analysis I.*, Tankönyvkiadó, Budapest, 1989 (in Hungarian).

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

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

4. I. M. James, *The topology of Stiefel manifolds*, Cambridge University Press, Cambridge, 1976.

5. V. V. Praszolov, *Linear algebra*, Typotex Kiadó, Budapest, 2005 (in Hungarian).

6. J. Radon, *Lineare Scharen orthogonaler Matrizen*, Abh. Sem. Hamburg 1 (1923), 1-14.

7. A. Rényi, *Combinatorial applications of finite geometries I.*, Mat. Lapok 17 (1966), 33-76 (in Hungarian).

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

9. M. Ujvári, *New descriptions of the Lovász number, and the weak sandwich theorem*, submitted to Pure Math. Appl. (2009).

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

Recent Operations Research Reports

2003-01 Zsolt Csizmadia and Tibor Illés: New criss-cross type algorithms for linear complementarity problems with sufficient matrices

2003-02 Tibor Illés and Ádám B. Nagy: A sufficient optimality criteria for linearly constrained, separable concave minimization problems

2004-01 Tibor Illés and Marianna Nagy: The Mizuno–Todd–Ye predictor–corrector algorithm for sufficient matrix linear complementarity problem

2005-01 Miklós Ujvári: On a closedness theorem

2005-02 Faluközy Tamás és Vizvári Béla: Az árutőzsde gabona szekciójának árvárakozásai a kukorica kereskedésének tükrében

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 Ujvári Miklós: Simplex-type algorithm for optimizing a pseudo-linear quadratic fractional function over a polytope

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

2007-01 Ujvári Miklós: 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