A Walsh-Fourier approach to the circulant Hadamard conjecture

Máté Matolcsi

Abstract We describe an approach to the circulant Hadamard conjecture based on Walsh-Fourier analysis. We show that the existence of a circulant Hadamard matrix of order n is equivalent to the existence of a non-trivial solution of a certain homogenous linear system of equations. Based on this system, a possible way of proving the conjecture is proposed.

1 Introduction

A *real Hadamard matrix* is a square matrix with ± 1 entries such that the rows (and thus the columns, also) are pairwise orthogonal. A *circulant (or cyclic) matrix C* is a square matrix which is generated by the cyclic permutations of a row vector, i.e. there exists a vector $\mathbf{x} = (x_1, \dots x_n)$ such that $c_{i,j} = x_{j-i+1}$ for $1 \le i, j \le n$ (the difference being reduced mod n to the set $\{1, \dots, n\}$; we prefer to use the indices $1, \dots, n$ rather than $0, \dots, n-1$).

It is trivial to check that the 4×4 circulant matrix generated by the row vector $(-1, 1, 1, 1)$ is Hadamard. However, no circulant Hadamard matrix of order larger than 4 is known. The following famous conjecture was made by Ryser [4], more than 50 years ago :

Conjecture 1. (Circulant Hadamard conjecture) For $n > 4$ there exists no $n \times n$ circulant real Hadamard matrix.

The first significant result concerning this conjecture was made by R. J. Turyn [7] using arguments from algebraic number theory. He proved that if a circulant Hadamard matrix of order n exists then n must be of the form $n = 4u^2$ for some odd

M. Matolcsi
Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences POB 127 H-1364 Budapest, Hungary, e-mail: matolcsi.mate@renyi.mta.hu

integer u which is not a prime-power. The most powerful breakthroughs were later obtained by the "field descent method" of B. Schmidt [5, 6] and its extensions by K. H. Leung and B. Schmidt [1, 2]. Currently, the smallest open case is $n = 4u^2$ with $u = 11715$, and there are less than 1000 remaining open cases in the range $u \leq 10^{13}$.

In this note we offer a more elementary approach to the circulant Hadamard conjecture, based on Walsh-Fourier analysis.

2 A Walsh-Fourier approach

The approach described in this note is inspired by the results of [3], where a Fourier analytic approach to the problem of mutually unbiased bases (MUBs) was presented. The basic idea is that the Fourier transform is capable of turning non-linear conditions into linear ones.

We briefly introduce the necessary notions and notations here. Let $\mathbb{Z}_2$ denote the cyclic group of order 2, and let $\mathscr{G} = \mathbb{Z}_2^n$. An element of $\mathscr{G}$ will be regarded as a column vector of length n whose entries are ± 1. And vice versa, each such column vector with ± 1 entries will be regarded as an element of $\mathscr{G}$. Accordingly, an $n \times n$ matrix A containing ± 1 entries will be regarded as an n-element subset of $\mathscr{G}$, the columns of A being the elements. We will use (Walsh)-Fourier analysis on $\mathscr{G}$. Let $\hat{\mathscr{G}}$ denote the dual group. Then $\hat{\mathscr{G}}$ is isomorphic to $\mathbb{Z}_2^n$ and an element γ of $\hat{\mathscr{G}}$ will be identified with a row vector containing 0-1 entries. The action of a character $\gamma = (\gamma_1, \dots \gamma_n) \in \hat{\mathscr{G}}$ on an element $\mathbf{x} = (x_1, \dots x_n) \in \mathscr{G}$ is defined as $\gamma(\mathbf{x}) = \mathbf{x}^\gamma = x_1^{\gamma_1} \dots x_n^{\gamma_n}$. We will also use the notation $\hat{\mathscr{G}}_0$ for the subgroup of elements $\gamma \in \hat{\mathscr{G}}$ such that $\gamma_1 + \gamma_2 + \cdots + \gamma_n \equiv 0 \pmod 2$.

In this note we will only use a few elements of discrete Fourier analysis on $\mathscr{G}$ and $\hat{\mathscr{G}}$, as follows. For any function $h : \mathscr{G} \to \mathbb{C}$ its Fourier transform is defined as $\hat{h}(\gamma) = \sum_{\mathbf{x} \in \mathscr{G}} h(\mathbf{x}) \mathbf{x}^\gamma$ for all $\gamma \in \hat{\mathscr{G}}$. For a function $f : \hat{\mathscr{G}} \to \mathbb{C}$ its Fourier transform is defined as $\hat{f}(\mathbf{x}) = \sum_{\gamma \in \hat{\mathscr{G}}} f(\gamma) \mathbf{x}^\gamma$ for all $\mathbf{x} \in \mathscr{G}$. The convolution of two functions $f, g : \hat{\mathscr{G}} \to \mathbb{C}$ is defined as $f * g(\gamma) = \sum_{\rho \in \hat{\mathscr{G}}} f(\gamma - \rho) g(\rho)$. Applying these definitions it is straightforward to verify that $\widehat{f * g}(\mathbf{x}) = \hat{f}(\mathbf{x}) \hat{g}(\mathbf{x})$ for every $\mathbf{x} \in \mathscr{G}$. Note also that $\hat{\mathscr{G}}$ is isomorphic to $\mathbb{Z}_2^n$, thus $\gamma - \rho = \gamma + \rho$ for each $\gamma, \rho \in \hat{\mathscr{G}}$, and therefore the convolution of f and g can also be written as $f * g(\gamma) = \sum_{\rho \in \hat{\mathscr{G}}} f(\gamma + \rho) g(\rho)$ (we will use this observation in equation (8) below).

Let A be any $n \times n$ matrix containing ± 1 entries, and let $\mathbf{a}_1, \dots, \mathbf{a}_n$ denote the columns of A. As explained above, we identify A with the subset $\{\mathbf{a}_1, \dots, \mathbf{a}_n\} \subset \mathscr{G}$, and actually further identify it with the indicator function of this subset. Therefore, the Fourier transform of (the indicator function of) A is given as $\hat{A}(\gamma) = \sum_{j=1}^n \mathbf{a}_j^\gamma$. Notice here that

$$|\hat{A}(\gamma)|^2 = \sum_{j,k=1}^{n} (\mathbf{a}_j / \mathbf{a}_k)^\gamma, \tag{1}$$

where the quotient $\mathbf{a}_j/\mathbf{a}_k$ is understood coordinate-wise, i.e. $\mathbf{a}/\mathbf{b} = (a_1/b_1, \dots, a_n/b_n)$. (As long as we work with ± 1 entries the operation division can be replaced by multiplication, but we prefer to use division in the notation because it can also be used in the more general context of complex Hadamard matrices.)

To illustrate the use of the Fourier transform $\hat{A}(\gamma)$, let me include here a neat proof of the fact that an $n \times n$ Hadamard matrix can only exist if 4 divides n. There is an easy combinatorial proof of this fact, but the Fourier proof is also very elegant.

Proposition 1. *If an $n \times n$ real Hadamard matrix exists, then 4 divides n, or $n = 1, 2$.*

Proof. Let H be an $n \times n$ real Hadamard matrix. If $n > 1$ then n must clearly be even. Assume $2|n$, but n is not divisible by 4.

As described above, the columns $\mathbf{h}_1, \dots \mathbf{h}_n$ of H can be regarded as elements of $\mathscr{G} = \mathbb{Z}_2^n$ and for any $0-1$ vector $\gamma \in \hat{\mathscr{G}}$ we have $\hat{H}(\gamma) = \sum_{j=1}^n \mathbf{h}_j^\gamma$,and

$$|\hat{H}(\gamma)|^2 = \sum_{j,k=1}^n (\mathbf{h}_j/\mathbf{h}_k)^\gamma. \tag{2}$$

Clearly, $|\hat{H}(\gamma)|^2 \geq 0$ for all γ. However, consider the element $\gamma = (1, 1, \dots, 1)$. On the right hand side of (2), within the summation we have $(\mathbf{h}_j/\mathbf{h}_k)^\gamma = 1$ if $j = k$, and $(\mathbf{h}_j/\mathbf{h}_k)^\gamma = -1$ if $j \neq k$ (here we use the fact that 4 does not divide n). Therefore, the right hand side evaluates to $n - n(n-1) = -n(n-2)$, which is negative if $n > 2$, a contradiction. □

Let us now turn to circulant Hadamard matrices. Assume $\mathbf{u} = (u_1, \dots u_n)$ is a ± 1 vector which which generates a circulant Hadamard matrix H. Consider the function

$$M(\gamma) = \mathbf{u}^\gamma \tag{3}$$

where γ ranges over $\hat{\mathscr{G}} = \mathbb{Z}_2^n$. Let $\pi_j \in \hat{\mathscr{G}}$ denote the element with an entry 1 at coordinate j, and all other entries being 0. Note that $M(\pi_j) = u_j$.

We have the following properties of the function M:

$$M(\gamma) = \pm 1 \text{ for all } \gamma \in \mathbb{Z}_2^n, \text{ and } M(0) = 1. \tag{4}$$

This is trivial.

For all $d = 1, \dots, n/2$, and all $\gamma \in \mathbb{Z}_2^n$ we have

$$\sum_{j-k=d (mod\ n)} M(\gamma + \pi_j + \pi_k) = 0. \tag{5}$$

This is a consequence of the cyclic orthogonality property: $\sum_{j=1}^n u_j u_{j+d} = 0$. Spelling it out:

$$\sum_{j-k=d (mod\ n)} M(\gamma + \pi_j + \pi_k) = \sum_{j=1}^n \mathbf{u}^{\gamma + \pi_j + \pi_{j+d}} = \mathbf{u}^\gamma \sum_{j=1}^n u_j u_{j+d} = 0.$$

The aim is to get a contradiction from the facts (4), (5) for $n > 4$. If we just consider the conditions (5), and regard each $M(\gamma)$ as a *real variable* then we have a homogenous system of linear equations with 2^n variables and $\frac{n}{2}2^n$ linear constraints. We will prove that this is an equivalent formulation of the circulant Hadamard conjecture, i.e. the existence of any non-trivial solution to this linear system of equations implies the existence of a circulant Hadamard matrix of order n. We will first need some intermediate lemmas.

Lemma 1. *The circulant Hadamard conjecture is true for n if and only if the n-variable equation*

$$\sum_{d=1}^{n-1}\left(\sum_{j=1}^{n} u_j u_{j+d}\right)^2 = 0 \tag{6}$$

admits no such solution where each variable u_j assumes ± 1 value.

Proof. This is trivial. □

While the above lemma is trivial, it can be combined with the system of equations (5). Let $S : \hat{G}_0 \to \mathbb{R}$ denote the function defined by the coefficients on the left-hand side of (6), i.e.

$$\sum_{d=1}^{n-1}\left(\sum_{j=1}^{n} u_j u_{j+d}\right)^2 = \sum_{\rho} S(\rho)\mathbf{u}^{\rho}. \tag{7}$$

Note that we have used the simplification $u_j^2 = 1$ (for each j) on the left hand side, so that indeed only monomials of the form $\mathbf{u}^{\rho}$ with $\rho \in \hat{\mathscr{G}}$ will appear on the right. Note that the right hand side can also be written as $\sum_{\rho} S(\rho)M(\rho)$.

Similar to (5) we can now write a system of linear equations involving S: if $\mathbf{u}$ generates a cyclic Hadamard matrix then $M(\gamma) = \mathbf{u}^{\gamma}$ satisfies the following equations:

$$\sum_{\rho} M(\gamma+\rho)S(\rho) = M(\gamma)\sum_{\rho} M(\rho)S(\rho) = 0 \text{ for all } \gamma \in \mathbb{Z}_2^n. \tag{8}$$

Keep in mind here that we will regard the values of M as real variables (disregarding the fact that M must be ± 1-valued). Therefore, there are 2^n variables and we have also 2^n the linear equations (one for each $\gamma \in \hat{\mathscr{G}}$, as given in (8)). This linear system leads to a coefficient matrix of size $2^n \times 2^n$. Any row in the coefficient-matrix will contain the same numbers $S(\rho)$, but the position of $S(\rho)$ is shifted according to the geometry of $\hat{\mathscr{G}} = \mathbb{Z}_2^n$. We will now show that the existence of a circulant Hadamard matrix of order n is equivalent to the coefficient-matrix being singular.

Lemma 2. *Regard each $M(\gamma)$ as a real variable, and consider the homogenous system of linear equations determined by* (8). *There exists a* ± 1 *vector* $\mathbf{u}$ *generating a cyclic Hadamard matrix if and only if* (8) *admits a non-trivial solution $M(\gamma)$.*

Proof. If $\mathbf{u}$ generates a cyclic Hadamard matrix then $M(\gamma) = \mathbf{u}^{\gamma}$ satisfies (8), yielding a non-trivial solution. In the converse direction, assume $M(\gamma)$ is a non-trivial solution to (8). That is, M is not identically 0, but we do not assume that M is ± 1-valued. Notice that the left hand side of (8) is the convolution $M * S$ of the functions M and S on the group $\hat{\mathscr{G}}$. This means that the convolution $M * S \equiv 0$ on $\hat{\mathscr{G}}$. Taking Fourier transform we conclude that $\widehat{M * S}(\mathbf{x}) = \hat{M}(\mathbf{x})\hat{S}(\mathbf{x}) = 0$ for every $\mathbf{x} \in \mathscr{G}$. As M is not identically zero, its Fourier transform cannot be identically zero either. Hence there exists an $\mathbf{u} \in \mathscr{G}$ such that $\hat{M}(\mathbf{u}) \neq 0$ and therefore $\hat{S}(\mathbf{u}) = \sum_\rho S(\rho)\mathbf{u}^\rho = 0$. By (7) this means exactly that there exist a solution $\mathbf{u}$ to the equation (6). □

We can now prove that the linear system of equations (5) is also an equivalent formulation of the circulant Hadamard conjecture.

Lemma 3. *Regard each $M(\gamma)$ as a real variable, and consider the homogenous system of linear equations determined by* (5)*. The circulant Hadamard conjecture is true for n if and only if this system of equations has full rank, i.e. the only solution is $M(\gamma) = 0$ for each γ.*

Proof. One direction is trivial: if $\mathbf{u}$ generates a circulant Hadamard matrix then $M(\gamma) = \mathbf{u}^\gamma$ is a non-trivial solution to (5).

Conversely, if there exists a non-trivial solution $M(\gamma)$ of (5) then M is a fortiori a solution of (8), because each equation in (8) is a linear combination of some equations in (5). Therefore a circulant Hadamard matrix exists by Lemma 2. □

While all the results above are fairly trivial, they do have some *philosophical* advantages. First, we can rest assured that Ryser's circulant Hadamard conjecture can be proved or disproved in this manner – we have not lost any information by setting up the system (5). Second, the circulant Hadamard conjecture is a non-existence conjecture, which can now be transformed to an existence result (i.e. it is enough to exhibit a *witness* which proves the non-existence of circulant Hadamard matrices):

Corollary 1. *The circulant Hadmard conjecture is true for n if and only if there exist real weights $c_{\gamma,d}$ such that*

$$\sum_{\gamma,d} c_{\gamma,d} \left(\sum_{j-k=d (mod\ n)} M(\gamma + \pi_j + \pi_k) \right) = M(0) \tag{9}$$

Proof. If such weights exist, then (5) cannot admit a solution in which $M(0) = 1$, and hence there cannot exist a circulant Hadamard matrix of order n. Conversely, if such weights do not exist then the linear system (5) does not have full rank, so a circulant Hadamard matrix of order n exists by Lemma 3. □

Therefore we are left with the "simple" task of exhibiting a witness (a set of weights $c_{\gamma,d}$) for each n. It is possible to obtain such witnesses by computer for small values of n, i.e. $n = 8, 12, 16, 20, 24$. The problem is that there are always an infinite number of witnesses (a whole affine subspace of them with large dimension), and one should somehow select the "nicest" one, which could be generalized for any n.

It is natural to exploit the invariance properties of the problem as follows. If $M(\gamma)$ is a non-trivial solution to (5) then so is $M_\pi(\gamma) = M(\pi(\gamma))$ where π is any cyclic permutation of the coordinates. We can therefore define equivalence classes in $\hat{\mathscr{G}}$, regarding γ_1 and γ_2 equivalent if they are cyclic permutations of each other. After averaging we can then assume that the required weights $c_{\gamma,d}$ are constant on equivalence classes. Furthermore, if $1 \leq k \leq n-1$ is relatively prime to n then multiplication by k defines an automorphism of the cyclic group $\mathbb{Z}_n$. We can regard γ_1 and γ_2 equivalent if a coordinate transformation corresponding to multiplication by some k transforms one to the other. Similarly, we can regard d_1 and d_2 equivalent if GCD(d_1,n)=GCD(d_2,n). After averaging again, we can assume that the required witness weights $c_{\gamma,d}$ depend only on the equivalence class of γ and that of d. However, such restrictions still do not determine the weights $c_{\gamma,d}$ uniquely, and still the witnesses form an affine subspace of large dimension.

It is also easy to see that we may restrict our attention without loss of generality to the subgroup $\hat{\mathscr{G}}_0 = \{\gamma \in \hat{\mathscr{G}} : \sum_{j=1}^n \gamma_j \equiv 0 \ (mod\ 2)\}$, because all the terms on the left hand side of (5) stay in $\hat{\mathscr{G}}_0$ if $\gamma \in \hat{\mathscr{G}}_0$. We will call $\sum_{j=1}^n \gamma_j$ the *weight* of γ, and denote it by $|\gamma|$.

In the last section of this note we will consider *symmetric* polynomials of the variables u_j, i.e. expressions of the form

$$\sum_{2|w=0}^{n} \sum_{|\gamma|=w} d_w M(\gamma). \tag{10}$$

That is, only $\gamma \in \hat{\mathscr{G}}_0$ are considered in the sum, and the coefficient of $M(\gamma)$ depends on the weight of γ only. It is trivial to see that if $M(\gamma) = \mathbf{u}^\gamma$ then (10) is a symmetric polynomial of $u_1, \ldots, u_n$. Expressions of the form (10) constitute a vector space of dimension $\frac{n}{2}+1$, a natural basis of which is given by the single-weight expressions

$$\sum_{|\gamma|=w} M(\gamma), \quad w = 0,2,4,\ldots n. \tag{11}$$

One way to generate an expression of the form (10) using the equations (5) is the following:

$$\sum_{|\gamma|=w} \sum_{d=1}^{n/2} \sum_{j-k=d(mod\ n)} M(\gamma + \pi_j + \pi_k), \quad w = 0,2,4,\ldots n. \tag{12}$$

Lemma 4. *If* 4 *divides n then the dimension of the subspace spanned by the expressions* (12) *in the vector space of the expressions of the form* (10) *is* $\frac{n}{2}+1$ *if* $n \neq 4u^2$, *while it is* $\frac{n}{2}$ *if* $n = 4u^2$.

Proof. For any $2 \leq w \leq n-2$ the left hand side of the expression (12) will contain variables $M(\gamma)$ where the weight $|\gamma|$ is $w-2, w$ or $w+2$. For $w = 0$ we will have γ's with weight $0,2$, while for $w=n$ we will have γ's with weight $n-2,n$. Therefore, it is easy to express (12) in the basis (11) explicitly, as a vector of length $\frac{n}{2}+1$ with only three non-zero coordinates for $2\leq w\leq n-2$ and only two non-zero coordinates for $w=0$ and $w=n$. This leads to a tri-diagonal coefficient matrix whose rank is $\frac{n}{2}+1$ if $n\neq 4u^2$, while it is $\frac{n}{2}$ if $n=4u^2$. The explicit calculations are left to the reader. □

This lemma leads to the following well-known corollary:

Lemma 5. *If there exists a cyclic Hadamard matrix of order n then n must be an even square number, $n=4u^2$.*

Proof. By Proposition 1 n must be divisible by 4. If $n\neq 4u^2$ then by Lemma 4 we see that the expressions (12) generate the whole space of symmetric polynomials given by (10). In particular, the single variable $M(0)$ (being a symmetric polynomial in itself) is also in this subspace, so we conclude that there exists an expansion of the form

$$\sum_{|\gamma|=w} c_w \sum_{d=1}^{n/2} \sum_{j-k=d(mod\ n)} M(\gamma+\pi_j+\pi_k)=M(0), \tag{13}$$

which is a special case of (9). □

One might object that this is a very difficult way of proving a very easy statement. However, it does have some advantages. First, it rhymes very well with (9) and the strategy described in the paragraphs after Lemma 1. Namely, put the γ's and the d's into some equivalence classes and look for a solution to (9) such that the coefficients depend only on the equivalence classes. Second, it "nearly" works even if n is a square: the span of the expressions (12) has dimension $\frac{n}{2}$. One could therefore hope for the following strategy to work. Let us call a linear combination on the left hand side of (13) "trivial". If we could find a non-trivial linear combination (9) such that the result is of the form (10), then it is "very likely" that the dimension of the span would increase to $\frac{n}{2}+1$, which would complete the proof of the general case. It is not at all clear whether such "magic" non-trivial linear combination is easy to find for general n, but it is not out of the question.

Acknowledgements The author was supported bt OTKA grant No. 109789 and by ERC-AdG 321104. This paper is in final form and no similar paper has been or is being submitted elsewhere.

References

1. Leung, K. H., Schmidt, B.: The field descent method. Des. Codes Cryptogr. **36**, 171–188 (2005)
2. Leung, K. H., Schmidt, B.: New restrictions on possible orders of circulant Hadamard matrices. Des. Codes Cryptogr. **64**, 143–151, (2012)
3. Matolcsi, M., Ruzsa, I. Z., Weiner, M.: Systems of mutually unbiased Hadamard matrices containing real and complex matrices. Australasian J. Combinatorics, **55** 35–47, (2013)

4. Ryser, H. J.: Combinatorial Mathematics. Wiley, New York (1963)
5. Schmidt, B: Cyclotomic integers and finite geometries. J. Amer. Math. Soc. **12**, 929–952, (1999)
6. Schmidt, B: Towards Ryser's Conjecture. In: C. Casacuberta et al. (eds) Proceedings of the Third European Congress of Mathematics, Progress in Mathematics **201**, pp. 533-541. Birkhuser, Boston (2001)
7. Turyn, R. J.: Character sums and difference sets. Pacific J. Math. **15**, 319–346 (1965)