A NOTE ON THE CIRCULANT HADAMARD CONJECTURE

M. MATOLCSI

ABSTRACT. This note reports work in progress in connection with Ryser's conjecture on circulant Hadamard matrices.

1. INTRODUCTION

We describe a general Fourier analytic approach to Ryser's conjecture on circulant Hadamard matrices.

Let me begin with stating the conjecture. For this we need two well-known notions. A *real Hadamard matrix* is a square matrix with ± 1 entries such that the rows (and thus columns) are pairwise orthogonal. A *cyclic (or circulant) matrix* C is a matrix which comes from the cyclic permutations of a row vector, i.e. there exists a vector $\mathbf{x} = (x_1, \dots x_n)$ such that $c_{i,j} = x_{j-i+1}$ (the difference being reduced mod n to the set $\{1, \dots, n\}$) for $1 \leq i, j \leq n$.

Conjecture 1.1. (Ryser) *For $n > 4$ there exists no $n \times n$ cyclic real Hadamard matrix.*

It is easy to check that for $n = 4$ there exists indeed a cyclic real Hadamard matrix. The conjecture is also known to be true for certain values of n, in particular for $4 < n < 10^{11}$ with three possible exceptions [1, 2].

2. A WALSH-FOURIER APPROACH

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

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. The Fourier transform of (the indicator function of) A will be defined as $\hat{A}(\gamma) = \sum_{j=1}^n \gamma(\mathbf{a}_j) = \sum_{j=1}^n \mathbf{a}_j^\gamma$. This is our main object of study. 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 division here can be replaced by multiplication, but i prefer to use division because it can also be used for 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 it always seemed a bit "ad hoc" to me. I believe that the Fourier proof is the "book proof".

Proposition 2.1. *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. As described above, the columns $\mathbf{h}_1, \dots \mathbf{h}_n$ of H can be regarded as elements of $\mathcal{G} = \mathbb{Z}_2^n$ and for any $0 - 1$ vector $\gamma \in \hat{\mathcal{G}}$ we have $\hat{H}(\gamma) = \sum_{j=1}^n \mathbf{h}_j^\gamma$,and

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

The function $\hat{H}(\gamma)$ is not invariant under the permutation of coordinates of γ, so let us consider the function

$$G_H(\gamma) = \sum_{\pi \in S_n} |\hat{H}(\pi(\gamma))|^2, \tag{3}$$

where π ranges through all permutations.

Observe that although we have no information on the specific columns of H, we still know the function G_H precisely, as described in the sequel. This is the main idea in this note. Let *Bal* denote the set of balanced vectors in $\mathbb{Z}_2^n$, containing the same number of $+1$ and -1 entries. Notice that the quotient $\mathbf{h}_j/\mathbf{h}_k$ of any two columns of H is either balanced (if $j \neq k$) or contains only 1s (if $j = k$). Therefore, in equation (2) we have terms of the form $\mathbf{u}^\gamma$ where $\mathbf{u}$ is balanced, and we have some trivial terms equal to 1. Furthermore, as π ranges over all permutations, each balanced vector gets included the same number of times, and hence

$$G_H(\gamma) = \sum_{\pi \in S_n} |\hat{H}(\pi(\gamma))|^2 = nn! + \frac{n(n-1)n!}{\binom{n}{n/2}} \sum_{\mathbf{u} \in Bal} \mathbf{u}^\gamma. \tag{4}$$

Also, the function G_H is clearly nonnegative, $G_H(\gamma) \geq 0$. Assume now by contradiction that $n = 2k$, k being odd. Let us evaluate $G_H(\gamma)$ at the vector $\gamma = (1, 1, \dots, 1)$. Each term $\mathbf{u}^\gamma$ on the right hand side of (4) equals -1 because k is odd. Therefore $G_H(\gamma) = nn! - n(n-1)n!$, which is clearly negative if $n > 2$, a contradiction. □

Let me now turn to Ryser's conjecture. Assume H is an $n \times n$ cyclic real Hadamard matrix. It is well-known that any cyclic Hadamard matrix (complex or real) is unbiased to the Fourier matrix F_n given by $[F_n]_{j,k} = e^{2i\pi(j-1)(k-1)/n}$, for $1 \leq j, k \leq n$. This means that for any column $\mathbf{f}$ of F_n and any column $\mathbf{h}$ of H we have $|\langle \mathbf{f}, \mathbf{h} \rangle| = \sqrt{n}$. (Remark: in particular, considering the first column $\mathbf{f}_1$ of F_n (containing only 1s) it follows that n must be a perfect square. This is well-known but we will not use this fact in this note.)

Assume $\mathbf{u} = (u_1, \dots u_n)$ is a ± 1 vector which which generates a cyclic Hadamard matrix. Consider the function

$$M(\gamma) = \mathbf{u}^\gamma \tag{5}$$

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

It is easy to see the following properties of M:

$$M(\gamma) = \pm 1 \text{ for all } \gamma \in \mathbb{Z}_2^n, \text{ and } M(0) = 1. \tag{6}$$

This is trivial.

And we have the following tiling equations for every $d = 1, \dots n/2$.

$$\sum_{j-k=d (mod\ n)} M(\gamma + \pi_j + \pi_k) = 0 \text{ for all } \gamma \in \mathbb{Z}_2^n. \tag{7}$$

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 these facts for $n > 4$.

So, how can we hope to get a contradiction?

First, there is a chance using linear algebra: there are 2^n variables $M(\gamma)$ (recall that γ ranges over $\hat{\mathcal{G}}$), and there are $\frac{n}{2}2^n$ linear constraints coming from (7). It seems likely that these conditions have full rank, so that the only solution to them is $M(\gamma) = 0$ for all γ, yielding a contradiction.

Second, there is a combinatorial possibility: one could hope to exploit the fact that M is known to be ± 1-valued. This leads us to an "anti-ham-sandwich" problem. For all $d = 1, \dots, n/2$ let $C_d \subset \hat{\mathcal{G}}$ denote the set of γ's with exactly two 1's which are d positions apart (mod n). Then equation (7) can be written as

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

In simple terms, we have $n/2$ different "domino-shapes" $C_1, \dots, C_{n/2}$, and we put these dominos to every position γ in the dyadic cube $\hat{\mathcal{G}}$, and we want to find a set $P \subset \hat{\mathcal{G}}$ (this is to be the set where $M(\gamma) = +1$) such that P cuts each domino exactly in half. This is a ham-sandwich problem, except that we want to prove that such P does not exist. That's why I call it an anti-ham-sandwich problem.

How can we prove that such a set P does not exist? I can imagine one way. It combines linear algebra with combinatorics. Assume there is a set W (which will be our witness), such that W has an odd number of elements and its indicator function χ_W can be tiled by our dominos, i.e. $\chi_W = \sum_{j,d} c_{j,d}\chi_{\gamma_j+C_d}$ for some constants $c_{j,d}$ and some positions γ_j and dominos C_d. This would lead to a contradiction because after applying the function M, the right hand side becomes 0 by equation (8) whereas the left-hand side cannot be zero due to parity reasons.

For example, for $n = 8, 12, 16$ one can set $W = \{0\}$ (a one-element set, containing only the origin). Then one can ask the computer to give a linear combination of the dominos that cancel out everywhere except at 0. Such a combination exists (indeed, the dominos span the whole space, so anything can be given as a linear combination of them; it is just natural to try out the indicator function of $\{0\}$, because one can hope that the coefficients will be nice and can be generalized for larger n). In fact, there are infinitely many solutions (because the linear system is highly degenerate: $\frac{n}{2}2^{n-1}$ vectors span a 2^{n-1}-dimensional space), and i don't know how to ask the computer to show me the nicest one.

Also, other choices of W are very well possible.

3. Minor results

I can report only a few minor results.

First i show that we do not lose information with this approach. That is, if Ryser's conjecture is true for some n, it can also be seen via this approach – in principle.

Lemma 3.1. *Regard each $M(\gamma)$ as a variable, and consider the system of linear equations determined by* (7). *Ryser's 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 $M(\gamma) = 0$ is the only solution then Ryser is true for n. To prove the other direction we need some further lemmas.

Lemma 3.2. *Ryser's conjecture is true for n if and only if the n-variable equation*

$$\sum_{d=1}^{n-1}\left(\sum_{j=1}^{n} u_j u_{j+d}\right)^2 = 0 \tag{9}$$

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

Proof. This is trivial. □

While the above lemma is trivial, it has the advantage of combining the "dominoes" into one super-domino. Let $S : \hat{G}_0 \to \mathbb{R}$ denote the function defined by the coefficients on the left-hand side of (9), i.e.

$$\sum_{d=1}^{n-1}\left(\sum_{j=1}^{n} u_j u_{j+d}\right)^2 = \sum_{\gamma} S(\gamma)\mathbf{u}^{\gamma}. \tag{10}$$

Similar to (7) 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:

$$\sum_{\rho} M(\gamma+\rho)S(\rho)=0 \text{ for } \text{ all } \gamma\in\mathbb{Z}_2^n. \tag{11}$$

Lemma 3.3. *There exists a* **u** *generating a cyclic Hadamard matrix if and only if the system of linear equations* (11) *admits a non-trivial solution.*

Proof. If **u** generates a cyclic Hadamard matrix then $M(\gamma)=\mathbf{u}^\gamma$ satisfies (11). In the converse direction, assume $M(\gamma)$ is a non-trivial solution to (11). It means that $S*M\equiv 0$ on $\hat{\mathcal{G}}$. Taking Fourier transform again, it means that $\hat{S}$ must have a zero on $\mathcal{G}$, which means exactly that there exist a solution **u** to the equation (9). □

We can now conclude the proof of Lemma 3.1. Indeed, if there is a non-trivial solution $M(\gamma)$ of (7) then M is a fortiori a solution of (11), and therefore a cyclic Hadamard matrix exists. □

All this is pretty trivial, but it has some *philosophical* advantages. First, we can rest assured that Ryser's conjecture can be proved or disproved in this manner. Second, the system of equations (11) leads to a square matrix. All we need to do is to prove that it is non-singular... of course this is very elusive. Last, and most importantly, Ryser's conjecture is a non-existence result, and it can now be transformed to an existence result (i.e. it is enough to exhibit a *witness* which proves the non-existence result):

Lemma 3.4. *Ryser's conjecture is true for n if and only if there exists real weights $c_{\gamma,d}$ such that*

$$\sum_{\gamma,d} c_{\gamma,d}\left(\sum_{j-k\equiv d(mod\ n)} M(\gamma+\pi_j+\pi_k)\right)=M(0) \tag{12}$$

Proof. This is now obvious. If such weights exist, then (7) cannot admit a solution in which $M(0)=1$, and hence there cannot exist a cyclic Hadamard matrix of order n. Conversely, if such weights do not exist then the linear system (7) (and also (11)) does not have full rank, so a cyclic Hadamard of order n exists. □

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 get 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 subspace of them with huge dimension), and one should somehow select the 'nicest' one, which somehow could be generalized for any n. I could not do this so far. There is a possibly promising idea here, exploiting the invariance properties of the problem as follows.

If $M(\gamma)$ is a non-trivial solution to (7) 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 $\hat{\mathcal{G}}$, 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, the same trick can be applied once more as follows. If $1 \le k \le n-1$ 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 dominoes C_{d_1} and C_{d_2} equivalent if GCD(d_1, n)=GCD(d_2, n). After averaging again, we can therefore assume that the required witness weights $c_{\gamma,d}$ depend only on the equivalence class of γ and that of d. Remark: in computer programming for small values of n i included the cyclic equivalences in the code, but not yet the multiplication equivalences. They may help.

Let me conclude this note with another minor result here. From the approach above it is not at all obvious why n should be a square number. We can prove it in the following way.

Lemma 3.5. *If there exists a cyclic Hadamard matrix of order n then n must be an even square number.*

Proof. It is trivial from equation (7) that n must be even, because otherwise the dominoes C_d would have an odd size and could not be cut in half (in fact, we implicitly assumed in (7) that n is even, otherwise d should run from 1 to $n-1$). It remains to prove that n is a square.

For a fixed $\gamma \in \hat{\mathcal{G}}$ sum up equation (7) for $d = 1, \dots \frac{n}{2}$ to obtain

$$\sum_{j \neq k} M(\gamma + \pi_j + \pi_k) = 0. \tag{13}$$

We will now form equivalence classes of the γ's different from the ones in the previous paragraph. Let $|\gamma|$ denote the number of 1's in γ (i.e. the *weight* of γ). Consider γ_1 and γ_2 equivalent if $|\gamma_1| = |\gamma_2|$. Suppose we multiply equation (13) by some coefficient $c_{|\gamma|}$ depending only on the weight of γ. When we sum everything up, it is easy to see that we will again obtain an equation where the coefficients depend only on the weight of γ, namely:

$$\sum_{w=0}^{n}\sum_{|\gamma|=w} c_w \sum_{j\neq k} M(\gamma+\pi_j+\pi_k) = \sum_{w=0}^{n}\sum_{|\gamma|=w} q_w M(\gamma). \tag{14}$$

So, the input is a distribution of weights c_w and the output is another distribution of weights d_w, for $w = 0, \dots n$. Clearly, this transformation is linear so it is described by a matrix T of size $(n+1)\times(n+1)$. It is easy to calculate the entries of T explicitly. It turns out that T has rank $n+1$ if n is not a square, and n if n is a square (i skip the calculations here). Therefore, if n is not a square then the matrix is of full rank and we can arrange the input weights c_w so that the output is $d_0 = 1$ and $d_w = 0$ otherwise. In other words the right hand side of (14) becomes $M(0)$, a contradiction since both sides of (14) are equal to 0 due to (13). □

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 (12) and the strategy described in the paragraphs after Lemma 3.4. Namely, put the γ's and the dominoes C_d into some equivalence classes and look for a solution to (12) such that the coefficients depend only on the equivalence classes. Second, it 'nearly' works even if n is not a square: the matrix T has rank n. One could therefore hope for the following to work. Let us call a linear combination on the left hand side of (12) 'trivial' if it arises in the form of the left hand side of (14). If we could find a non-trivial linear combination (12) such that the result is of the form $\sum_{w=0}^{n}\sum_{|\gamma|=w} q_w M(\gamma)$ (i.e. the coefficients depend only on the weight of γ), then it is 'very likely' that joining this new equation as a new row of T, the rank would increase to $n+1$ and we would be done.

References

[1] B. Schmidt, *Cyclotomic integers and finite geometries.* J. Amer. Math. Soc. 12 (1999) 929-952.

[2] B. Schmidt, *Towards Ryser's Conjecture.* Proceedings of the Third European Congress of Mathematics (eds C. Casacuberta et al.), Progress in Mathematics 201 (Birkhuser, Boston, 2001) 533-541.

M. M.: Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences POB 127 H-1364 Budapest, Hungary Tel: (+361) 483-8307, Fax: (+361) 483-8333

E-mail address: matomate@renyi.hu