



HAL
open science

Ryser's Conjecture and Stochastic matrices

Luis H Gallardo

► **To cite this version:**

| Luis H Gallardo. Ryser's Conjecture and Stochastic matrices. 2024. <hal-04582304>

HAL Id: hal-04582304

<https://hal.science/hal-04582304v1>

Preprint submitted on 21 May 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons CC BY 4.0 - Attribution - International License

Ryser's Conjecture and Stochastic matrices

Luis H. Gallardo
UMR CNRS 6205

Laboratoire de Mathématiques de Bretagne Atlantique
6, Av. Le Gorgeu, C.S. 93837, Cedex 3, F-29238 Brest
France

`Luis.Gallardo@univ-brest.fr`

2020 Mathematics Subject Classification: Primary 15B34;
Secondary: 11A05

Keywords: Circulant matrices, Hadamard matrices, stochastic matrices.

Abstract

Assume that H is a circulant Hadamard matrix of order $n \geq 4$. We consider an appropriate stochastic matrix S of order n depending on H . This allows us to prove that $n = 4$. Thus, there are only 10 circulant Hadamard matrices.

1 Introduction

A matrix of order n is a square matrix with n rows. A *circulant* matrix $A := \text{circ}(a_1, \dots, a_n)$ of order n is a matrix of order n , with first row $[a_1, \dots, a_n]$, in which each row after the first is obtained by a cyclic shift of its predecessor by one position. For example, the second row of A is $[a_n, a_1, \dots, a_{n-1}]$. Three useful circulant matrices of order n are the matrix J with all its entries equal to 1, i.e., $J := \text{circ}(1, \dots, 1)$, the identity matrix $I := \text{circ}(1, 0, \dots, 0)$, and the zero matrix $0 := \text{circ}(0, \dots, 0)$. A *Hadamard* matrix H of order n is a matrix of order n with entries in $\{-1, 1\}$ such that $K := \frac{H}{\sqrt{n}}$ is an orthogonal matrix with rational entries. A *circulant Hadamard* matrix of order n is a circulant matrix that is Hadamard of order n . The

10 known circulant Hadamard matrices are $H_1 := \text{circ}(1)$, $H_2 := -H_1$, $H_3 := \text{circ}(1, -1, -1, -1)$, $H_4 := -H_3$, $H_5 := \text{circ}(-1, 1, -1, -1)$, $H_6 := -H_5$, $H_7 := \text{circ}(-1, -1, 1, -1)$, $H_8 := -H_7$, $H_9 := \text{circ}(-1, -1, -1, 1)$, $H_{10} := -H_9$. A *stochastic* matrix S of order n is a matrix of order n with non-negative entries such that the sum of all entries of each row of S is equal to 1. If the transpose of S is also stochastic, then S is a *doubly stochastic* matrix. We denote by A^* the conjugate transpose of the matrix A . When A has real entries A^* is simply the transpose of A .

Ryser proposed in 1963 (see [2, p. 97], [8]) the conjecture of the non-existence of circulant Hadamard matrices of order > 4 . Ryser's conjecture has since attracted some attention, see, e.g., [1, 3, 4, 9] and their bibliographies.

Brualdi [1], a student of Ryser, proved the conjecture for every order n provided H is symmetric, and Turyn [9] proved the conjecture for all n 's of the form $n = 4p^{2m}$ where p is an odd prime number and m is a positive integer. Turyn [9, pp. 329-330] also proved the crucial fact that $n = 4h^2$ with *odd* h .

The object of the present paper is to prove the conjecture. It turns out that this follows immediately when we focus on the following doubly stochastic matrix S (see Lemma 3), associated to a circulant Hadamard matrix H of order $4h^2$.

$$S := \frac{H + J}{2(2h^2 + h)}. \quad (1)$$

The link with the OEIS sequence A091704 (see [7]) is the following. If Ryser's Conjecture holds then there is no Barker codes of length > 13 (see [10]).

Our main result is the following.

Theorem 1. *There is no circulant Hadamard matrices with more than 4 rows.*

Section 2 contains some results useful for the proof of the theorem. The proof of the theorem appears in section 3.

2 Tools

The following is well known. See, e.g., [5, p. 1193], [6, p. 234], [9, pp. 329-330].

Lemma 2. *Let H be a regular Hadamard matrix of order $n \geq 4$, i.e., a Hadamard matrix whose row and column sums are all equal. Then $n = 4h^2$ for some positive integer h . Moreover, the row and column sums are all equal to $\pm 2h$ and each row has $2h^2 \pm h$ positive entries and $2h^2 \mp h$ negative entries. Finally, if H is circulant then h is odd.*

A simple computation follows.

Lemma 3. *Let $H := \text{circ}(h_1, \dots, h_n)$ be a circulant Hadamard matrix of order n . Then, the matrix $S := \frac{H+J}{n+\sqrt{n}}$ is circulant and doubly stochastic.*

Proof. By Lemma 2 $n = 4h^2$. Sums and scalar multiples of circulant matrices are circulant. Thus, both $H + J$ and S are circulant. Put s the sum of all entries in any row of S . By Lemma 2 we can assume that the sum r of all entries in any row of $H + J$ is equal to $2h + 4h^2$ (if not we change H into $-H$). Since $n + \sqrt{n} = 2(2h^2 + h)$ we obtain that $s = 1$. Thus S is stochastic. Since $(H + J)^* = H^* + J^* = H^* + J$, and

$$H^* + J = \text{circ}(h_1 + 1, h_n + 1, h_{n-1} + 1, \dots, h_2 + 1) \quad (2)$$

the sum of all entries in any row of $H^* + J$ is also equal to r . Thus S^* is stochastic. This proves that S is doubly stochastic. \square

3 Proof of Theorem 1

Assume that H is a circulant Hadamard matrix with at least 4 rows, i.e, H has order $n \geq 4$. By Lemma 2 $n = 4h^2$ with odd h . We can assume (if not we replace H by $-H$) that there are $\frac{n+\sqrt{n}}{2} = 2h^2 + h$ entries equal to 1 in row 1 of H (see Lemma 2). By Lemma 3 the matrix S defined in (1) is circulant and doubly stochastic. It follows from (1) that

$$H = 2h(2h + 1)S - J. \quad (3)$$

Computing the transpose conjugate in both sides of (3) we get

$$H^* = 2h(2h + 1)S^* - J. \quad (4)$$

since J is real and symmetric. But H is Hadamard so that

$$nI = HH^*. \quad (5)$$

Using (5) together with (3) and (4); using that I, J, H, H^*, S, S^* are all circulant so that any product of two of them commute, and using that $J^2 = nJ$ we obtain the following equality:

$$4h^2I = 4h^2(2h + 1)^2SS^* - 2h(2h + 1)(S + S^*)J + 4h^2J. \quad (6)$$

But $SJ = J$ and $S^*J = J$ since S is doubly stochastic. Thus, dividing both sides of (6) by h we get

$$4hI = 4h(2h + 1)^2SS^* - 4(2h + 1)J + 4hJ. \quad (7)$$

Reducing both sides of (7) modulo h we obtain

$$0 = -4J \pmod{h}. \quad (8)$$

Therefore, (8) says that

$$h \mid 4. \quad (9)$$

But h is odd by Turyn's result in Lemma 2. Thus, (9) implies that

$$h = 1. \quad (10)$$

In other words, we have proved that $n = 4$. This proves the theorem.

References

- [1] R. A. Brualdi, A note on multipliers of difference sets, *J. Res. Nat. Bur. Standards Sect. B* **69** (1965), 87–89.
- [2] P. J. Davis, *Circulant matrices, 2nd ed.*, New York, NY: AMS Chelsea Publishing, xix, 250 p., 1994.
- [3] L. H. Gallardo, New duality operator for complex circulant matrices and a conjecture of Ryser, *Electron. J. Combin.* **23** (2016), no. 1, Paper 1.59, 10 pp.
- [4] L. H. Gallardo, Under a mild condition Ryser's conjecture holds for every $n = 4h^2$ with h odd and non square-free, *Math. Commun.* **26**, (2021), no. 1, 1–8.
- [5] A. Hedayat and W.D. Wallis, Hadamard matrices and their applications, *Ann. Statist.* **6** (1965), no. 6, 1184–1238.

- [6] D. B. Meisner, On a construction of regular Hadamard matrices, *Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lince* **9**, *Mat. Appl.* **3**, no. 4, (1992), 233–240.
- [7] N. J. A. Sloane et al., *The On-Line Encyclopedia of Integer Sequences*, published electronically at <https://oeis.org>, 2019.
- [8] H. J. Ryser, *Combinatorial mathematics. The Carus Mathematical Monographs, No. 14.* , Published by The Mathematical Association of America; distributed by John Wiley and Sons, Inc., New York, xiv+154 pp 1963.
- [9] R. J. Turyn, Character sums and difference sets, *Pac. J. Math.* **15** (1965), 319–346.
- [10] Wikipedia: Barker code