ABELIAN SUBGROUP OF $O_4(\mathbb{Q})$ RELATED TO RYSER’S CONJECTURE

LUIS H. GALLARDO

Abstract. We characterize the group generated by the $4 \times 4$ circulant Hadamard matrices divided by 2.

1. Introduction

A matrix of order $n$ is a square matrix with $n$ rows. A circulant matrix $A := \text{circ}(a_1, \ldots, a_n)$ of order $n$ is a matrix of order $n$, with first row $[a_1, \ldots, a_n]$, in which each row after the first is obtained by a cyclic shift to the right of its predecessor by one position. For example, the second row of $A$ is $[a_n, a_1, \ldots, a_{n-1}]$.

A Hadamard matrix $H$ of order $n$ is a matrix of order $n$ with entries in $\{-1, 1\}$ such that $K := H/\sqrt{n}$ is an orthogonal matrix with rational entries $\pm 1/\sqrt{n}$. Seminal papers on Hadamard and modular Hadamard matrices include [2, 3, 14, 15].

A circulant Hadamard matrix of order $n$ is a circulant matrix that is Hadamard. The 10 known circulant Hadamard matrices are $H_a := \text{circ}(1)$, $H_b := -H_a$, and

$$
H_1 := \text{circ}(1, 1, 1, -1), \quad H_{1n} := -H_1, \quad H_2 := \text{circ}(-1, 1, 1, 1), \quad H_{2n} := -H_2, \quad (1.1)
$$

$$
H_3 := \text{circ}(1, -1, 1, 1), \quad H_{3n} := -H_3, \quad H_4 := \text{circ}(1, 1, -1, 1), \quad H_{4n} := -H_4. \quad (1.2)
$$

Put for $j = 1, \cdots, 8$, $K_j := H_j/2$. We will compute and characterize the abelian subgroup $G_4$ of the orthogonal group $O_4(\mathbb{Q})$, generated by $K_1, \ldots, K_8$.

If $H = \text{circ}(h_1, \ldots, h_n)$ is a circulant Hadamard matrix of order $n$ then its representer polynomial is the polynomial $R(x) := h_1 + h_2x + \cdots + h_nx^{n-1}$.

No one has been able, despite several deep computations (see [22]), to discover any other circulant Hadamard matrix. Ryser proposed in 1963 (see [5, p. 97], [28]) the conjecture of the non-existence of these matrices when $n > 4$. Ryser’s conjecture has since attracted many attention [1, 7, 8, 9, 10, 11, 12, 19, 20, 21, 22, 24, 26, 30].

One of the most important and deep results on the conjecture are Schmidt and Leung results [19, 20, 21], obtained by developing new algebraic tools related to cyclotomic fields and group algebras [13]. These work helped Logan and Mossinghoff [22] to obtain the nice result that up to order $4 \cdot 10^{30}$ there are only 4489
undecided values of $n$ (thus the Conjecture holds for very large orders). Frames
[27] are important tools for another approach to the conjecture as well.

For an $n \times n$ Hadamard matrix $H$, a much more simpler, and well known,
sufficient condition to prove Ryser’s conjecture (see Proposition 2.8) is that $K :=
H/\sqrt{n}$ have only algebraic integers as eigenvalues or equivalently that $K$ has finite
order in $O_n(\mathbb{Q})$. Exploiting this observation, we are able to prove the following
result that is our main result, and the object of the present paper.

More precisely, our main result is the following:

**Theorem 1.1.** Let $G_n$ be the subgroup of $O_n(\mathbb{Q})$ generated by all matrices of the
form $K := H/\sqrt{n}$ where $H$ is an $n \times n$ circulant Hadamard matrix, where $n \geq 4$.
Let $L_n$ be a finite subgroup of circulant matrices of $O_n(\mathbb{Q})$ with $|L_n| \leq 2n + 1$.
Assume that $G_n$ is discrete. Then $R_n := G_n \times L_n$ is isomorphic to $G_4$; i.e., $n = 4,$
and $R_n \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

See Section 2 for the necessary tools for the proof of the theorem. Section 3
contains the proof of Theorem 1.1. For a matrix $M$ with complex entries, we
let $M^*$ denote the transpose conjugate matrix of $M$. Also, we let $I_k$ denote the
identity matrix of order $k$. For a finite set $S$, as usual, we let $|S|$ denote the
number of elements of $S$.

Observe that our reduction method transform the matrix problem into a prob-
lem about finite order subgroups of a classical group, here the orthogonal group
over the rational numbers. Previous useful work in the more general case of non-
abelian subgroups includes [18, 29], and in our specific case the work of [6] (see
Lemma 2.7) is crucial.

2. Tools

The following is well known. See, e.g., [17, p. 1193], [25, p. 234], [30, pp.
329-330] for the first lemma and [5, p. 73] for the second.

**Lemma 2.1.** Let $H$ be a regular Hadamard matrix of order $n \geq 4$. Then $n = 4h^2$
for some positive integer $h$. Moreover, if $H$ is circulant then $h$ is odd. Furthermore,
either $H$ or $-H$ is $2h$–regular (the other is $(-2h)$–regular) and each row
has $2h^2 + h$ positive entries and $2h^2 - h$ negative entries, when $H$ is $2h$–regular;
respectively, has $2h^2 - h$ positive entries and $2h^2 + h$ negative entries, when $H$
is $(-2h)$–regular.

**Lemma 2.2.** Let $H$ be a circulant Hadamard matrix of order $n$, let $w = \exp(\frac{2\pi i}{n})$
and let $R(x)$ be its representer polynomial. Then all the eigenvalues $R(v)$ of $H$,
where $v \in \{1, w, w^2, \ldots, w^{n-1}\}$, satisfy

$$|R(v)| = \sqrt{n}.$$  

More generally and in more detail (see [5]) one has

**Lemma 2.3.** Let $C = \text{circ}(c_1, \ldots, c_n)$ be a circulant matrix of order $n > 0$ with
representer polynomial $P(t) = c_1 + c_2 t + \ldots + c_n t^{n-1}$. Let $\omega$ be the primitive complex
$n$-th root of unity with smaller positive argument. The matrix $C$ is diagonalizable
and $C = F^* \Delta F$ where $\Delta = \text{diag}(P(1), P(w), \ldots, P(w^{n-1}))$ is a diagonal matrix
containing the eigenvalues of $C$ and $F^* = \left( \frac{\omega^{(i-1)(j-1)}}{\sqrt{n}} \right)$ is the conjugate of the Fourier matrix. Moreover, $F$ is unitary.

We recall the classical result of Kronecker (see for example, [16, pages 97-98]) and its special case of cyclotomic extensions (see e.g., [16, Theorem 8.1.10 a]).

**Lemma 2.4.** (a) The only algebraic integers all whose conjugates lie on the unit circle are the roots of unity.

(b) Let $n > 0$ be an even positive integer. Let $K = \mathbb{Q}(w)$, where $w$ is a primitive $n$-th root of 1, be a cyclotomic extension of the rational numbers. The only algebraic integers in $K$ all whose conjugates lie on the unit circle belong to \{1, w, \ldots, w^{n-1}\}.

The next lemma is [23, Theorem 3], see also [4, Theorem 3.1]. It was already used in [9, 11].

**Lemma 2.5.** Let $A$ be a circulant matrix of order $n > 0$ with entries in \{0,1\}. Let $J$ be the circulant matrix of order $n$ that has all its entries equal to 1. Let $m$ be an even positive integer. Assume that $A^m \in \mathbb{Z}I + \mathbb{Z}J$. Then $A \in \{0, P, J, J-P\}$, where $P$ is a permutation matrix of order $n$.

Craigen and Kharaghani [4, Lemma 4] proved part (a) of the following lemma, as a consequence of Lemma 2.1 and Lemma 2.5. Part (b) of the following lemma, is (a trivial), but useful reformulation of the case $n > 1$ of part (a).

**Lemma 2.6.** Let $H$ be a circulant Hadamard matrix of order $n \geq 1$.

(a) Assume that for some positive number $m$, $H^m = n^m I$. Then $n \leq 4$.

(b) Assume that $n > 1$. Let $K := H/\sqrt{n}$. Assume that for some positive number $m$, the orthogonal matrix $K$ has multiplicative order $m$. Then $n = 4$.

**Proof.** Part (a) follows from [4, Lemma 4]. From the hypothesis of (b) we have that $m$ is even and that $K^m = I$. Thus

$$H^m = (\sqrt{n})^m I = n^m I.$$  \hfill (2.1)

The result follows then from (a). \hfill \Box

The following lemma follows from [6, Theorem 2].

**Lemma 2.7.** Let $G \subseteq GL_n(\mathbb{Q})$ be a finite abelian group. One has

(a) $|G| \leq 6^{\frac{3}{2}}2^{n-2}\frac{5}{2}$,

(b) $|G| \leq 3^{\frac{3}{2}}$, if $2 \nmid |G|$,

(c) $|G| \leq 2^n$, if $3 \nmid |G|$.

The following proposition states the sufficient condition required by our argument.
Proposition 2.8. Let \( n := 4h^2 \) with \( h \geq 1 \) odd. Let \( H \) be an \( n \times n \) circulant Hadamard matrix, and let \( K \in O_n(Q) \) with entries in \( \{ \pm \frac{1}{\sqrt{n}} \} \). Then \( K \in O_n(Q) \) with entries in \( \{ \pm \frac{1}{\sqrt{n}} \} \), the cyclic subgroup of \( O_n(Q) \) generated by \( K \), and \( \omega := \exp(\frac{2\pi i}{n}) \), the following statements hold.

(a) \( G_0 \) finite implies \( n = 4 \).

(b) \( K \) has all its eigenvalues in the ring of integers \( \mathbb{Z}[\omega] \) of the cyclotomic field \( \mathbb{Q}(\omega) \), implies \( n = 4 \).

(c) Let \( G_n \) be the subgroup of \( O_n(Q) \) generated by all circulant matrices of the form \( K = \frac{H_n}{\sqrt{n}} \) where \( H \) is an \( n \times n \) circulant Hadamard matrix. Then \( G_n \) discrete implies \( n = 4 \).

Proof. Part (a) follows from Lemma 2.6 (b). Part (b) follows from Lemma 2.4. Since a discrete subgroup of the orthogonal group \( O_n(Q) \) is finite, part (c) follows from part (a). \( \square \)

The following lemma computes the group \( G_4 \) generated by all \( 4 \times 4 \) circulant Hadamard matrices. Computations checked in gp-PARI.

Lemma 2.9. Following Davis [5, p. 67] we put \( \pi := \text{circ}(0,1,0,0) \). With the above notations the subgroup \( G_4 \) of \( O_4(Q) \) generated by all \( K_j \)'s for \( j = 1, \ldots, 8 \), contains 16 elements:

\[
G_4 := \{ I_4, K_1, K_1^2, K_2, K_1^3 K_2, K_3, K_4, -K_1^2, K_4^2, K_4^3, K_2 K_1, K_2, K_1 K_2 \} \cup \\
\{ K_1 K_4, (K_1 K_4)^3, K_1 K_3 \},
\]

where

\[
K_1 = (1/2)\text{circ}(1,1,1,-1), K_1^2 = \pi^2 = \text{circ}(0,0,1,0), \\
K_2 = \pi K_1 = (1/2)\text{circ}(-1,1,1,1), \\
K_3 = \pi K_2 = (1/2)\text{circ}(1,-1,1,1), K_4 = \pi K_3 = (1/2)\text{circ}(1,1,-1,1), \\
-K_1^2 = -\pi^2 = \text{circ}(0,0,-1,0), K_1^3 K_2 = K_3 K_2 = \pi = \text{circ}(0,1,0,0), \\
K_4 = -K_4 = (1/2)\text{circ}(-1,-1,1,-1), K_4^3 = -K_3 = (1/2)\text{circ}(-1,1,-1,-1), \\
K_2 = -K_2 = (1/2)\text{circ}(1,-1,-1,-1), K_1 = -K_1 = (1/2)\text{circ}(-1,-1,-1,-1), \\
K_1 K_2 = \pi^3 = \text{circ}(0,0,0,1), K_1 K_4 = -\pi = \text{circ}(0,-1,0,0), \\
(K_1 K_4)^3 = -\pi^3 = -K_1 K_2 = \text{circ}(0,0,0,-1), K_1 K_3 = -I_4
\]

Moreover, one sees that:

\[
G_4 \cong \{ I_4, -I_4 \} \times \{ I_4, \pi, \pi^2, \pi^3 \} \times \{ I_4, K_1 \},
\]
i.e.,

\[
G_4 \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}). \tag{2.2}
\]

The following lemma helps to complete the proof of the Theorem.

Lemma 2.10. The identity matrix \( I_4 := \text{circ}(1,0,0,0) \) is the unique circulant \( 4 \times 4 \) matrix \( A \in GL_4(Q) \) such that \( AF_4 = F_4 A \), where \( D \) is a diagonal matrix with complex entries, such that \( D^3 = I_4 \), and \( F_4 \) is the Fourier matrix \( F \) defined in Lemma 2.3, when \( n = 4 \).
Proof. Let \( \alpha \in \mathbb{C} \) be a 3-th root of unity unequal to 1; i.e., \( \alpha^2 = -\alpha - 1 \) in \( \mathbb{C} \). By a straightforward computation in gp-PARI, we obtained that the unique diagonal matrix \( D \) with diagonal \((a, b, c, d)\) where \( a, b, c, d \in \{1, \alpha, \alpha^2\} \) such that \( A = F_4 D F_4^* \) has rational entries (81 possibilities) is \( D = A = I_4 \). \( \square \)

3. Proof of Theorem 1.1

Since \( G_n \) is discrete, Proposition 2.8 (c) implies that \( n = 4 \), so that \( G_n = G_4 \). By Lemma 2.9 we have (2.2). It remains to prove that \( L_n = L_4 \) is reduced to the identity matrix. Put \( \ell_4 := |L_4| \). One has \( \ell_4 \leq 9 \). If \( \ell_4 \in \{1, 2, 4, 5, 7, 8\} \) then, by Lemma 2.7 applied to \( G_4 \times L_4 \) we obtain that \( |G_4 \times L_4| \leq 2^4 = 16 \), but \( |G_4 \times L_4| = 16\ell_4 \), thus \( \ell_4 = 1 \). If \( \ell_4 \in \{3, 6, 9\} \) then \( L_4 \) has an element of order 3. This is not possible by Lemma 2.10. The result follows.

Acknowledgement. We are grateful to the referee and the editor for nice suggestions.

References

12. L. H. Gallardo, Under a mild condition, Ryser’s Conjecture holds for every \( n := 4h^2 \) with \( h > 1 \) odd and non square-free, Math. Commun. 26, 2021, no. 1, 1–8.

1 Univ. Brest, UMR CNRS 6205, Laboratoire de Mathématiques de Bretagne Atlantique, F-29238 Brest, France.
Email address: Luis.Gallardo@univ-brest.fr