Hacettepe Journal of Mathematics and Statistics
Volume 43 (2) (2014), 227 – 230

A shorter proof of the Smith normal form of skew-Hadamard matrices and their designs

İlhan Hacıoğlu* and Aytül Keman†

Abstract

We provide a shorter algebraic proof for the Smith normal form of skew-hadamard matrices and the related designs.

Keywords: p-rank, Hadamard design, Smith normal form.

2000 AMS Classification: 20C08, 51E12, 05B20

1. Introduction

Smith normal forms and *p-ranks* of designs can help distinguish non-isomorphic designs with the same parameters. So it is interesting to know their Smith normal form explicitly. Smith normal forms of some designs were computed in [2],[3] and [5]. In this article we give a shorter proof for the Smith normal form of skew-hadamard matrices and their designs.

A *Hadamard matrix* H of order n is an n by n matrix whose elements are ± 1 and which satisfies $HH^T = nI_n$. It is *skew-Hadamard matrix* if, it also satisfies $H + H^T = 2I_n$. For more information about the Hadamard matrices please see [1], [9]. Similar definitions stated below can be found in [4], [5], [6], [7], [8], [9].

The *incidence matrix* of a Hadamard $(4m-1, 2m, m)$ design D is a $4m-1$ by $4m-1$ $(0,1)$-matrix A that satisfies

$$AA^T = A^TA = mI + mJ.$$

The complementary design $\overline{D}$ is a $(4m-1, 2m-1, m-1)$ design with incidence matrix $J - A$. A skew-hadamard $(4m-1, 2m, m)$ design is a hadamard design that satisfies(after some row and column permutations)

$$A + A^T = I + J$$

*Department of Mathematics, Arts and Science Faculty Çanakkale Onsekiz Mart University, 17100 Çanakkale,Turkey, Email: `hacioglu@comu.edu.tr`

†Department of Mathematics, Arts and Science Faculty Çanakkale Onsekiz Mart University, 17100 Çanakkale,Turkey, Email: `aytulkeman@hotmail.com`

Integral Equivalence: If A and B are matrices over the ring Z of integers, A and B are called *equivalent* ($A \sim B$) if there are $Z-$matrices P and Q, of determinant ± 1, such that

$$B = PAQ$$

which means that one can be obtained from the other by a sequence of the following operations:

- Reorder the rows,
- Negate some row,
- Add an integer multiple of one row to another,

and the corresponding column operations.

Smith Normal Form: If A is any n by n, $Z-$ matrix, then there is a unique $Z-$matrix

$$S = diag(a_1, a_2, ..., a_n)$$

such that $A \sim S$ and

$$a_1|a_2|...|a_r, a_{r+1} = \ldots = a_n = 0,$$

where the a_i are non-negative. The greatest common divisor of i by i subdeterminants of A is

$$a_1 a_2 a_3 \ldots a_i.$$

The a_i are called *invariants factors* of A and S is the Smith normal form($SNF(A)$) of A.

***p*-Rank:** The *p-rank* of an n by n, $Z-$ matrix A is the rank of A over a field of characteristic p and is denoted by $rank_p(A)$. The p-rank of A is related to the invariant factors $a_1, a_2, ..., a_n$ by

$$rank_p(A) = max\{i : p \text{ does not divide } a_i\}$$

2. Proof of the main theorem

2.1. Proposition. ([6] or [8])*: Let H be a Hadamard matrix of order $4m$ with invariant factors $h_1, ..., h_{4m}$. Then $h_1 = 1$, $h_2 = 2$, and $h_i h_{4m+1-i} = 4m$ ($i = 1, \ldots, 4m$).*

2.2. Theorem. ([7])*: Let A, B, $C = A + B$, be n by n matrices over Z, with invariant factors $h_1(A)| \ldots |h_n(A)$, $h_1(B)| \ldots |h_n(B)$, $h_1(C)| \ldots |h_n(C)$, respectively. Then*

$$gcd(h_i(A), h_j(B)) | h_{i+j-1}(A + B)$$

for any indices i, j with $1 \leq i, j \leq n$, $i + j - 1 \leq n$, where gcd denotes greatest common divisor.

2.3. Theorem. ([4])*: Let D be a skew-Hadamard $(4m-1, 2m, m)$ design. Suppose that p divides m. Then $rank_p(D) = 2m - 1$ and $rank_p(\overline{D}) = 2m$.*

The author in [5] proves the following theorem by using completely different method. Here we provide a shorter algebraic proof for this theorem and the corollary following it.

2.4. Theorem. *A skew-Hadamard matrix of order $4m$ has Smith normal form*

$$diag[1, \underbrace{2, \ldots, 2}_{2m-1}, \underbrace{2m, \ldots, 2m}_{2m-1}, 4m].$$

Proof. Applying Theorem 2.2 with $A = H$ and $B = H^T$ we get $gcd(h_i(H), h_j(H^T))|2$ which means that $gcd(h_i(H), h_j(H^T)) = 1$ or 2 where $1 \leq i, j \leq 4m$, $i+j-1 \leq 4m$. If $m = 1$ then we have a skew-Hadamard matrix of order 4 and by proposition 1 the result follows. Assume that $m > 1$ then by proposition 1 we know that $h_1(H) = 1$, $h_2(H) = 2$, $h_{4m-1}(H) = 2m$ and $h_{4m}(H) = 4m$. Since $SNF(H) = SNF(H^T)$ assume that $h_{2m}(H) = 2k$ and $h_{2m}(H^T) = 2k$ where $k \neq 1$ and k is a divisor of m. In this case $i = j = 2m$ and Theorem 2.2 gives us $gcd(h_i(H), h_j(H^T)) = 2k|2$. But this is a contradiction since $k \neq 1$. So $k = 1$ which means that $h_{2m}(H) = h_{2m}(H^T) = 2$. So all the first $2m$ elements except the first one have to be 2. Since we found the first $2m$ elements, using proposition 1 again we obtain the remaining elements namely $h_{2m+1}(H) = h_{2m+2}(H) = \ldots = h_{4m-1}(H) = 2m$ and $h_{4m}(H) = 4m$. □

2.5. Corollary. *The Smith normal form of the incidence matrix of a skew-Hadamard $(4m-1, 2m, m)$ design is*

$$diag[\underbrace{1, \ldots, 1}_{2m-1}, \underbrace{m, \ldots, m}_{2m-1}, 2m].$$

Proof. By [5] any skew-Hadamard matrix of order $4m$ is integrally equivalent to $[1] \oplus (2A)$. This means that all the invariant factors of A are half of the corresponding invariant factors of H except the first one. So the result follows. □

Note that we know from Theorem 2.3 that $rank_p A = 2m - 1$ which agrees with our result.

By using similar techniques that we used above we get the Smith normal form of the complementary skew-Hadamard design:

2.6. Corollary. *The Smith normal form of the incidence matrix of a skew-Hadamard $(4m-1, 2m-1, m-1)$ design is*

$$diag[\underbrace{1, \ldots, 1}_{2m}, \underbrace{m, \ldots, m}_{2m-2}, m(2m-1)].$$

References

[1] Horadam, K.J. *Hadamard Matrices and their Applications*, Princeton University Press, Princeton, (2010).

[2] Koukouvinos, C., Mitrouli, M., Seberry, J. *On the Smith Normal form of D-optimal designs*, Linear Algebra Appl., 247, 277-295, (1996).

[3] Koukouvinos, C., Mitrouli, M., Seberry, J. *On the Smith Normal form of weighing matrices*, Bull. Inst. Combin. Appl., 19, 57-69, (1997).

[4] Michael, T.S. *The p-Ranks of Skew Hadamard Designs*, J. Combin. Theory, Ser.A 73, 170-171, (1996).

[5] Michael, T.S., Wallis, W.D. *Skew-Hadamard Matrices and the Smith Normal Form*, Designs, Codes and Cryptography 13, 173-176, (1998).

[6] Newman, M. *Invariant Factors of Combinatorial Matrices*, Israel J. Math. 10, 126-130, (1971).

[7] Thompson, R.C. *The Smith Invariants of a Matrix Sum*, Proc. Amer. Math. Soc. 78, 162-164, (1980).
[8] Wallis, W.D., Wallis, J. *Equivalence of Hadamard Matrices*, Israel J. Math. 7, 122-128, (1969).
[9] Wallis, W.D. *Combinatorial Designs*, Marcel Dekker, New York, (1988).