Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory
September 7–13, 2014, Svetlogorsk (Kaliningrad region), Russia *pp. 91–96*

On Hadamard Modulo Prime p Matrices of Size at most $2p + 1$ [1]

Yuri L. Borissov youri@math.bas.bg
Institute of Mathematics and Informatics, BAS, Sofia, 1113, Bulgaria
Moon Ho Lee moonho@chonbuk.ac.kr
Institute of Information and Communication, CBNU, Jeonju, 561-756, R. Korea

Abstract. In this note, we continue the study of Hadamard Modulo Prime (HMP) matrices initialized in recent articles [5] – [6]. Namely, we have present some new non-existence and classification results for HMP matrices whose size is relatively small with respect to the modulo.

1 Introduction

The HMP matrices could be considered in a wider context of modular Hadamard matrices (introduced in 1972 by Marrero and Butson [1]) whose concept has recently resurfaced in the engineering literature during the course of investigation of the so-called jacket matrices (see, [2]). In the present note, our main concern motivated by their remarkable cryptographic application, the so-called "all-or-nothing transforms" (AONT), is on the prime modular matrices. The reader is referred to [3] for the general concept of these transforms, and to [4] where it is pointed out for the first time how to construct linear AONT based on Hadamard matrices. The recent article [5] considers an extension of that method, while [6] is devoted to $5-$modular matrices.

The outline of this note is as follows. In the next section we remind some necessary definitions and preliminary facts, and in Section 4 we exhibit our results on HMP matrices of relatively small size.

2 Preliminaries

First, we recall the following definition.

Definition 1. *A HMP matrix* $\mathbf{H}$ *of size* n *modulo odd prime* p*, is an* $n \times n$ *non-singular over* $\mathbf{GF}(p)$ *matrix of* ± 1*'s such that*

$$\mathbf{H}\mathbf{H}^T = n(mod\, p)\, \mathbf{I}_n, \tag{1}$$

where $\mathbf{I}_n$ *is the identity matrix of size* n*.*

[1] This research is partially supported by MEST 2012-002521, NRF. Korea.

We shall use the notation $HMP(n,p)$ for the set of HMP matrices of size n modulo p.

Remark 1. *Although some authors do not impose invertibility on those matrices, we prefer to do because of the aforementioned application of corresponding linear transforms. Necessary and sufficient condition for that is the matrix size n is not a multiple of the chosen modulo p. So, in further we assume that $p \not| \; n$.*

Remark 2. *Evidently, each ordinary Hadamard matrix belongs to $HMP(n,p)$ for arbitrary prime $p > 2$. The simplest nontrivial example for HMP matrix is obtained when $n = 7$ and $p = 3$, e.g.,*

$$\begin{pmatrix} \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & - & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & - \\ \mathbf{1} & \mathbf{1} & - & \mathbf{1} & \mathbf{1} & \mathbf{1} & - \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & - & \mathbf{1} & \mathbf{1} & - \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & - & \mathbf{1} & - \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & - & - \\ \mathbf{1} & - & - & - & - & - & \mathbf{1} \end{pmatrix},$$

where $-$ has been written instead of -1.

Clearly, *Definition* 1 would be reformulated as follows. The matrix $\mathbf{H} \in HMP(.,p)$ if and only if the (real) inner product of every pair of distinct rows $\mathbf{h}'$ and $\mathbf{h}''$ of $\mathbf{H}$ equals to zero modulo p, i.e.:

$$(\mathbf{h}', \mathbf{h}'') \equiv 0 \; (mod \, p).$$

We remind as well an necessary condition for existence of odd size HMP matrix (see, e.g., [5]):

Proposition 1. *If the size n of HMP matrix modulo p is odd then $n(mod \; p)$ must be a quadratic residue modulo p.*

Definition 2. *The matrix $\mathbf{A}$ of $\pm 1s$ is called equivalent to the matrix $\mathbf{B}$ if the former is obtained from the latter by the following transformations:*

- *permuting the set of rows/columns of $\mathbf{B}$;*
- *multiplying each row (column) from a certain subset of rows (columns) in $\mathbf{B}$ with -1.*

Remark 3. *Clearly, the above defined transformations preserve the Hadamard property. Also, it is easy to show that when performing them one can apply at the beginning all permutations and then all transformations of the second kind.*

Definition 3. *The (Hamming) distance between two vectors* $\mathbf{x}$ *and* $\mathbf{y}$ *of equal length is the number of positions where they differ, and is denoted by* $dist(\mathbf{x}, \mathbf{y})$.

Definition 4. *The weight of a vector* $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ *where* $x_i \in \{1, -1\}$, *denoted by* $wt(\mathbf{x})$, *is the number of* $x_i = -1$. *The set* $S(\mathbf{x}) = \{i : x_i = -1\}$ *is called support of* $\mathbf{x}$.

It is easily seen that for any two vectors $\mathbf{x}$ and $\mathbf{y}$ of length n with components from the set $\{1, -1\}$, it holds: $(\mathbf{x}, \mathbf{y}) = n - 2dist(\mathbf{x}, \mathbf{y})$. Also, $wt(\mathbf{x}) = dist(\mathbf{x}, \mathbf{1})$ where $\mathbf{1}$ is the all-one vector.

We shall also make use of the following easy to prove lemmata.

Lemma 1. *(see, e.g., [7][Chapter 1, p. 19]) Define the intersection of two vectors* $\mathbf{x}$ *and* $\mathbf{y}$ *of* ± 1 *to be the vector* $\mathbf{x} * \mathbf{y}$ *of the same length which has* $-1s$ *only where both* $\mathbf{x}$ *and* $\mathbf{y}$ *do. Then it holds:*

$$dist(\mathbf{x}, \mathbf{y}) = wt(\mathbf{x}) + wt(\mathbf{y}) - 2wt(\mathbf{x} * \mathbf{y}). \tag{2}$$

Lemma 2. *For arbitrary two rows* $\mathbf{r}'$, $\mathbf{r}''$ *of an non-singular size* n *matrix of* ± 1*'s, their inner product obeys*

$$|(\mathbf{r}', \mathbf{r}'')| \leq n - 2.$$

3 HMP matrices of relatively small size

We start with the following proposition.

Proposition 2. *Let* $\mathbf{H} \in HMP(n, p)$ *where* $n \leq p + 1$. *Then* $\mathbf{H}$ *is an ordinary Hadamard matrix.*

Proof. Indeed, by *Lemma* 2 for arbitrary two distinct rows $\mathbf{h}'$, $\mathbf{h}''$ of $\mathbf{H}$, we have:

$$|(\mathbf{h}', \mathbf{h}'')| \leq n - 2 < p$$

But, since $(\mathbf{h}', \mathbf{h}'') \equiv 0 \ (mod\, p)$ then the only possibility is $(\mathbf{h}', \mathbf{h}'') = 0$. □

Corollary 1. *If* $p \equiv 1 (mod\ 4)$ *then the set* $HMP(p + 1, p)$ *is the empty one. In particular, there does not exist* $HMP(6, 5)$ *matrix.*

Proof. When $p \equiv 1 \ (mod\ 4)$ the existence of ordinary Hadamard matrix of size $n = p + 1$ contradicts the well-known fact that n must be 1, 2, or $n \equiv 0 (mod\ 4)$ (see, e.g., [8][Section 2.2]). □

Proposition 3. *Let* $\mathbf{H} \in HMP(n, p)$ *where* n *is an even number such that* $n < 2p$. *Then* $\mathbf{H}$ *is an ordinary Hadamard matrix.*

Proof. By *Lemma* 2 for the inner product of two arbitrary distinct rows $\mathbf{h}'$, $\mathbf{h}''$ of $\mathbf{H}$, we have:

$$|(\mathbf{h}', \mathbf{h}'')| \leq n - 2 < 2p - 2.$$

Hence, the only possible values of that product are $\pm p$ and 0. But, also since $(\mathbf{h}', \mathbf{h}'') = n - 2dist(\mathbf{h}', \mathbf{h}'')$, this inner product is of the same parity like n. This rejects the values $\pm p$, and the proof is completed. $\square$

Corollary 2. *If $2 < n < 2p$ and $n \equiv 2 (mod\ 4)$ then $HMP(n, p)$ is the empty set.*

Proposition 4. *Let $\mathbf{H} \in HMP(n, p)$ where n is an odd number such that $n \leq 2p + 1$, and let $\omega = (n - p)/2$. Then the matrix $\mathbf{H}$ is equivalent to a matrix $\mathbf{M}$ having the following three properties:*

(i) the first row of $\mathbf{M}$ is the all-one vector $\mathbf{1}$;

(ii) all remaining rows are of weight ω;

(iii) for arbitrary two distinct rows $\mathbf{r}'$ and $\mathbf{r}''$ of $\mathbf{M}$, it holds: $dist(\mathbf{r}', \mathbf{r}'') = \omega$.

In addition, $n - p \equiv 0\ (mod\ 4)$.

Proof. W.l.o.g. we may assume that the first row of $\mathbf{H}$ coincides with $\mathbf{1}$, and let $\mathbf{h}$ be its arbitrary other row. By *Lemma* 2, we have: $|(\mathbf{h}, \mathbf{1})| \leq n - 2 \leq 2p - 1$. Proceeding like in the proof of *Proposition* 3, we get that the inner product $(\mathbf{h}, \mathbf{1}) = n - 2wt(\mathbf{h}) \equiv 0 (mod\ p)$ has odd parity, and thus equals $\pm p$. So, $wt(\mathbf{h}) = (n \pm p)/2$. But, if for instance $wt(\mathbf{h}) = (n + p)/2$, we can multiply $\mathbf{h}$ by -1 making the weight of that row equal to $(n - p)/2 = \omega$. This proves (ii), i.e., $\mathbf{H}$ is equivalent to a matrix $\mathbf{M}$ whose rows (excluding the first) are of weight ω. By similar reasoning we can prove that matrix satisfies property (iii), too.

Now, we will prove the last claim. To this end, take two distinct rows $\mathbf{r}'$ and $\mathbf{r}''$ of $\mathbf{M}$ different from the first one. By *Lemma* 1 it holds:

$$\omega = dist(\mathbf{r}', \mathbf{r}'') = wt(\mathbf{r}') + wt(\mathbf{r}'') - 2wt(\mathbf{r}' * \mathbf{r}'') = 2\omega - 2wt(\mathbf{r}' * \mathbf{r}''),$$

thus $\omega = 2wt(\mathbf{r}' * \mathbf{r}'')$. Combining with $\omega = (n - p)/2$ the claim is deduced. $\square$

Remark 4. *The properties (iii) and (ii) of the matrix $\mathbf{M}$ mean that the binary code standing behind its rows is a equidistant constant weight code. The reader is referred to [9] for basic definitions on these codes and proof for the equivalence between the ordinary Hadamard matrices and certain constant weight codes.*

Corollary 3. *If $p \equiv 1 (mod\ 4)$ then the set $HMP(2p + 1, p)$ is the empty one. In particular, there does not exist $HMP(11, 5)$ matrix.*

Corollary 4. *The set $HMP(p+2l, p)$ where $l \equiv 1 (mod\ 2)$ and $0 < l \leq (p+1)/2$, is the empty set for arbitrary prime p.*

Remark 5. *Proposition 2 shows the nonexistence of $HMP(n, p)$ matrix with odd $n < p$. Putting $l = 1$ in Corollary 4 we conclude as well that $HMP(p+2, p)$ is the empty set for arbitrary p. This fact cannot be derived in all cases by Proposition 1, since 2 is a quadratic residue modulo p whenever $p \equiv \pm 1 (mod\ 8)$.*

Finally, we will consider the first possible case where a HMP matrix which is not ordinary Hadamard matrix may exist, i.e., the odd size $n = p + 4$. But, before stating the next theorem we introduce for convenience some terminology. A matrix of ±1's is said to be permutation ±1's matrix if each row/column contains exactly one -1. A permutation ±1's matrix with -1's entries over the main diagonal is called diagonal one.

Theorem 1. *Every $HMP(p+4, p)$ matrix is equivalent to the diagonal ±1's matrix*

$$\mathbf{D}_{p+4} = \begin{pmatrix} -1 & 1 & 1 & . & . & . & 1 \\ 1 & -1 & 1 & . & . & . & 1 \\ 1 & 1 & -1 & . & . & . & 1 \\ . & . & . & . & . & . & . \\ . & . & . & . & . & . & . \\ 1 & 1 & 1 & . & . & . & -1 \end{pmatrix}.$$

Proof. By *Proposition* 4, any $\mathbf{H} \in HMP(p+4, p)$ is equivalent to a matrix whose first row $\mathbf{h}_1$ is the all-one vector $\mathbf{1}$, while each other row $\mathbf{h}_k,\ k > 1$, is a vector with support of cardinality 2 and the intersection of every pair among these supports has just one element. We will show that all supports have an element in common. Of course, w.l.o.g. we may assume that $S(\mathbf{h}_2) = \{1, 2\}$ and $S(\mathbf{h}_3) = \{1, 3\}$. Suppose now that $1 \notin S(\mathbf{h}_4)$, then by necessity $S(\mathbf{h}_4) = \{2, 3\}$. Furthermore, for $S(\mathbf{h}_5)$ we have three possibilities: $S(\mathbf{h}_5) = \{e, 4\}$ where $e = 1, 2$ or 3. Let, for instance, $S(\mathbf{h}_5) = \{1, 4\}$. This implies $dist(\mathbf{h}_4, \mathbf{h}_5) = 4$, which contradicts *Proposition* 4(iii). The remaining two possibilities are rejected in the same way. So, the assumption $1 \notin S(\mathbf{h}_4)$ is not correct, and we may assume $S(\mathbf{h}_4) = \{1, 4\}$. Continue in this way we conclude that $S(\mathbf{h}_k) = \{1, k\}$ for any $1 < k \leq p + 4$. Finally, multiplying the first column by -1, we conclude that $\mathbf{H}$ is equivalent to $\mathbf{D}_{p+4}$. Obviously $\mathbf{D}_{p+4} \in HMP(p+4, p)$, which completes the proof. □

Theorem 2. *Let p be arbitrary odd prime and $n = p+4$. Then $|HMP(n, p)| = 2^{2n-1}\ n!$.*

Proof. Exhibiting the proof we stick to *Remark* 3. Since by *Theorem* 1 any $HMP(n, p)$ matrix is equivalent to the diagonal matrix $\mathbf{D}_n$ then applying permutations one will get only permutation $HMP(n, p)$ matrices. And, of course, any permutation ±1's matrix of size n can be obtained in this way, justifying the multiplier $n!$ in the above formula. The second type of equivalence transformations is specified by a pair of subsets of rows and columns, respectively. Thus, it provides another 2^{2n} possibilities. However, obviously the pair of complement subsets leads to the same matrix. Thus, the number of different matrices which can be obtained in this way is at most 2^{2n-1}. In fact, it turns out that number is exactly 2^{2n-1}, but we left the details of comprehensive rigorous proof for the reader. □

4 *Conclusion*

In this note, we have studied the set of HMP matrices of relatively small size, namely for a given prime $p > 2$ the set $HMP(n, p)$ where $n \leq 2p + 1$. First, we proved that the sets $HMP(n, p)$ with $n \leq p + 1$ and $HMP(n, p)$ with even $n < 2p$ contain only ordinary Hadamard matrices, if at all. Then we proved an new necessary condition for the existence of HMP matrices with odd size at most $2p+1$. Due to that, we showed that the sets $HMP(p+2, p)$ for arbitrary p and $HMP(2p+1, p)$ for $p \equiv 1(mod\, 4)$, are the empty set. The cases $n = p+1$ or $n = 2p + 1$ generalize facts pointed out in [6] for a particular value $p = 5$. Also, we have proved that up to equivalence there exists exactly one $HMP(p + 4, p)$ matrix and found the number of all equivalent matrices of that kind.

A careful analysis of the proofs of presented results shows that most of them remain valid for more common type of matrices having arbitrary odd modulo m which is co-prime to the size n when $n \leq 2m + 1$.

References

[1] O. Marrero and A. T. Butson, Modular Hadamard matrices and related designs, *J. Comb. Theory A* **15**, 257–269, 1973.

[2] M. H. Lee, A new reverse jacket transform and its fast algorithm, *IEEE Trans. Circuits Syst. II*, **47(6)**, 39–47, 2000.

[3] R. L. Rivest, All-or-nothing encryption and the package transform, in *Biham, E. (Ed.), Fast Software Encryption, Lect. Notes Comp. Sci. 1267*, 210–218, 1997.

[4] D. R. Stinson, Something about all or nothing (transforms), *Des. Codes Cryptogr.*, **22**, 133–138, 2001.

[5] M. H. Lee, Y. L. Borissov, and S. M. Dodunekov, Class of jacket matrices over finite characteristic fields, *Electron. Lett.*, **46(13)**, 916–918, 2010.

[6] M. H. Lee and F. Szollosi, Hadamard matrices modulo 5, *Journal of Combinatorial Designs*, 171–178, 2013.

[7] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes,* North-Holland, Amsterdam, 1977.

[8] V. D. Tonchev, *Combinatorial configurations: designs, codes, graphs,* Longman Wiley, New York, 1988.

[9] V. A. Zinoviev, On the equivalence of certain constant weight codes and combinatorial designs, *Journal of Statistical Planning and Inference*, **56**, 289–294, 1996.