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

Yuri Borissov

Institute of Mathematics and Informatics, BAS, Bulgaria

joint work with Moon Ho Lee

Chonbuk National University, R. of Korea

ACCT-14 Svetlogorsk, Russia 2014

Outline

- Introduction & Motivation

Outline

- Introduction & Motivation
- Preliminaries

Outline

- Introduction & Motivation
- Preliminaries
- Results and Sketch of Proofs

Definition 1.

A **Hadamard Modulo Prime** (HMP) matrix $\mathbf{H}$ of size n is an $n \times n$ non-singular over $\mathbb{Z}_p$, $p > 2$, matrix of ± 1's such that:

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

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

- Let $HMP(n, p)$ be the set of HMP modulo p matrices of size n.

- The HMP matrices could be considered in a wider context of modular Hadamard matrices introduced by Marrero and Butson in [MarBut72];

- The HMP matrices could be considered in a wider context of modular Hadamard matrices introduced by Marrero and Butson in [MarBut72];
- The concept has recently resurfaced in the engineering literature – jacket transforms (JT): introduced in [Lee00];

- The HMP matrices could be considered in a wider context of modular Hadamard matrices introduced by Marrero and Butson in [MarBut72];
- The concept has recently resurfaced in the engineering literature – jacket transforms (JT): introduced in [Lee00];
- The HMP matrices are applicable to constructing some linear all-or-nothing transforms (AONT) – a remarkable cryptographic technique for strengthening modern block ciphers: introduced in [Riv97], elaborated in [Sti01], and recently extended in [LeeBorDod10].

- Necessary and sufficient condition for invertibility of size n matrix with modular Hadamard property is that $p \nmid n$.

Preliminaries

- Necessary and sufficient condition for invertibility of size n matrix with modular Hadamard property is that $p \not| \, n$.
- Each ordinary real Hadamard matrix belongs to $HMP(n, p)$ for arbitrary prime $p > 2$, provided $p \not| \, n$.

- Necessary and sufficient condition for invertibility of size n matrix with modular Hadamard property is that $p \nmid n$.
- Each ordinary real Hadamard matrix belongs to $HMP(n,p)$ for arbitrary prime $p > 2$, provided $p \nmid n$.
- The simplest nontrivial example for HMP matrix is obtained when $n = 7$ and $p = 3$, e.g.,

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & - & 1 & 1 & 1 & 1 & - \\ 1 & 1 & - & 1 & 1 & 1 & - \\ 1 & 1 & 1 & - & 1 & 1 & - \\ 1 & 1 & 1 & 1 & - & 1 & - \\ 1 & 1 & 1 & 1 & 1 & - & - \\ 1 & - & - & - & - & - & 1 \end{pmatrix}.$$

Definition 2.

The matrix **A** is called **equivalent** to the matrix **B** of ± 1s when **A** can be obtained from **B** by the following transformations:

- permuting the set of rows/columns of **B**;
- multiplying each row/column from a certain subset of rows/columns in **B** by -1.

- When performing these transformations one can apply, firstly, all permutations, and then the transformations of 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, denoted by:

$$dist(\mathbf{x}, \mathbf{y}).$$

The **weight** of a vector $\mathbf{x}$ of ± 1, denoted by $wt(\mathbf{x})$, is $dist(\mathbf{x}, \mathbf{1})$ where $\mathbf{1}$ is the all-ones vector.

- For any two vectors $\mathbf{x}$ and $\mathbf{y}$ of ± 1's with length n, it holds:
$$(\mathbf{x}, \mathbf{y}) = n - 2dist(\mathbf{x}, \mathbf{y}).$$
In particular, the **inner product** of two vectors of ± 1's has the **same parity** as their common **length**.

Lemma 4.

The inner product of a pair of distinct rows of an non-singular size n matrix of ± 1's does not exceed in absolute value $n - 2$.

- ...

Lemma 4.

The inner product of a pair of distinct rows of an non-singular size n matrix of ± 1's does not exceed in absolute value $n - 2$.

- ...

Lemma 5.

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:

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

- *the* **intersection** *lemma*

Proposition 6.

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

- **Sketch of proof:** *Lemma* 4 implies the inner product of arbitrary two distinct rows of $\mathbf{H}$ equals 0.

Results: $HMP(n, p)$ $n \leq 2p + 1$ 1

Proposition 6.

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

- **Sketch of proof:** *Lemma* 4 implies the inner product of arbitrary two distinct rows of $\mathbf{H}$ equals 0.

Corollary 7.

If $p \equiv 1 (mod\ 4)$ *then the set* $HMP(p + 1, p)$ *is the empty one.*

- The corollary generalizes a result for particular case of $5-$modular matrices considered in [LeeSzo13].

I. Case $n \equiv 0 (mod\ 2)$.

Proposition 8.

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

- **Sketch of proof:** The inner product of each pair of rows is of **even parity** like n, and bounded in absolute value by $2p$. Hence, it vanishes.

I. Case $n \equiv 0 (mod\ 2)$.

Proposition 8.

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

- **Sketch of proof:** The inner product of each pair of rows is of **even parity** like n, and bounded in absolute value by $2p$. Hence, it vanishes.

Corollary 9.

If $2 < n < 2p$ *and* $n \equiv 2 (mod\ 4)$ *then* $HMP(n, p) = \emptyset$*.*

II. Case $n \equiv 1 (mod\ 2)$.

Proposition 10.

Let $\mathbf{H} \in HMP(n, p)$ *for odd* $n \leq 2p + 1$, *and* $\omega = (n - p)/2$.
$\mathbf{H}$ *is equivalent to a matrix* $\mathbf{M}$ *with the following properties:*

(i) *the first row of* $\mathbf{M}$ *is the all-ones vector* $\mathbf{1}$;
(ii) *all other rows are of weight* ω;
(iii) *for arbitrary two distinct rows* $\mathbf{r}'$ *and* $\mathbf{r}''$ *of* $\mathbf{M}$:

$$dist(\mathbf{r}', \mathbf{r}'') = \omega.$$

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

- **Idea of proof:** **(ii) – (iii)** are proved similarly to the previous proposition but now the inner product has **odd parity**. Finally, the last claim is deduced making use of the **intersection** lemma.

Corollary 11.

If $p \equiv 1 (mod\ 4)$ then the set $HMP(2p + 1, p)$ is the empty one.

The last fact generalizes a second result from [LeeSzo13]: Namely, there does not exist $HMP(11, 5)$ matrix.

Remarks

- Properties **(iii) – (ii)** mean the binary code behind the rows of the matrix **M** is an **equidistant constant weight** code;
- A theorem on the **equivalence** of an ordinary Hadamard matrix and a certain constant weight code was proved by V.A. Zinoviev in [Zin96].

- The odd size $n = p + 4$ is the **simplest** case s. t. a $HMP(., p)$ matrix which is **not** an ordinary Hadamard, may exist.

- The odd size $n = p + 4$ is the **simplest** case s. t. a $HMP(., p)$ matrix which is **not** an ordinary Hadamard, may exist.

Theorem 12.

Let $n = p + 4$ where p is an odd prime. Then:
(a) *Every $HMP(n,p)$ matrix is equivalent to $\mathbf{D}_n = \mathbf{J}_n - 2\mathbf{I}_n$, where $\mathbf{J}_n$ is the all-ones matrix.*
(b) *The cardinality of $HMP(n,p)$ equals to $2^{2n-1}\ n!$*

- The odd size $n = p + 4$ is the **simplest** case s. t. a $HMP(., p)$ matrix which is **not** an ordinary Hadamard, may exist.

Theorem 12.

Let $n = p + 4$ where p is an odd prime. Then:
(a) *Every $HMP(n, p)$ matrix is equivalent to $\mathbf{D}_n = \mathbf{J}_n - 2\mathbf{I}_n$, where $\mathbf{J}_n$ is the all-ones matrix.*
(b) *The cardinality of $HMP(n, p)$ equals to $2^{2n-1}\ n!$*

- **Idea of proof:** **(a)** follows by Proposition 10, while **(b)** is proved based on **(a)** and taking into consideration the peculiarities of equivalence transformations.

[MarBut72] O. Marrero and A. T. Butson,
Modular Hadamard matrices and related designs,
J. Comb. Theory A **15**, 257–269, 1973.

[Lee00] M. H. Lee,
A new reverse jacket transform and its fast algorithm,
IEEE Trans. Circuits Syst. II, **47(6)**, 39–47, 2000.

[Riv97] 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.

[Sti01] D. R. Stinson,
Something about all or nothing (transforms),
Des. Codes Cryptogr., **22**, 133–138, 2001.

[LeeBorDod10] 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.

[LeeSzo13] M. H. Lee and F. Szollosi,
Hadamard matrices modulo 5,
J. of Combinatorial Designs, 171–178, 2013.

[Zin96] V. A. Zinoviev,
On the equivalence of certain constant weight codes and combinatorial designs,
J. of Statistical Planning and Inference, **56**, 289–294, 1996.

The End

THANK YOU FOR ATTENTION!