

Comment on revised version of “The Hadamard circulant conjecture”

Robert Craigen

Jonathan Jedwab

15 November 2011

Abstract

The revised version of the claim by Hurley, Hurley and Hurley to have proved the circulant Hadamard matrix conjecture is mistaken.

In January 2011, Hurley, Hurley and Hurley [2] claimed to have proved the circulant Hadamard matrix conjecture, but the proof was mistaken [1]. In September 2011, a revised version [3] of the paper [2] was posted to the arXiv, with the comment that “This is post publication revision of on-line Bull. London Math. Soc. version which changes subsection 3.3.” We show that the revised version is also mistaken, by summarising part of the argument of [3] and then presenting a counterexample.

A *2-block* is a matrix of the form $D = \begin{bmatrix} i & j \\ j & i \end{bmatrix}$ for $i, j \in \{1, -1\}$, and is *even* if $i = j$ and *odd* if $i = -j$. Suppose there exists a circulant Hadamard matrix H of order $4n$. Reorder the rows and columns of H to form a $2n \times 2n$ matrix M whose entries are 2-blocks, as in [3, p.7], and write the first row of M as $[M_0 \ M_1 \ \dots \ M_{2n-1}]$. Then exactly n of the 2-blocks M_i are even, and

$$\sum_{i : M_i \text{ and } M_{i+u} \text{ are even}} M_i M_{i+u} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \quad \text{for each } u \neq 0, \quad (1)$$

where all matrix subscripts are reduced modulo $2n$. Fix $u \neq 0$. Then from (1), for each i such that M_i and M_{i+u} are even, we can assign a unique ℓ such that M_ℓ and $M_{\ell+u}$ are even and such that $M_\ell M_{\ell+u} = -M_i M_{i+u}$. We then also assign i to ℓ , write $(i, i+u) \sim (\ell, \ell+u)$, and call the index pairs $(i, i+u)$ and $(\ell, \ell+u)$ *matching*.

An even 2-block M_i is *symmetric* when the 2-block M_{i+n} is also even. The following argument is given [3, p.8] to claim that “every even block is symmetric” when $n > 1$. Suppose, for a contradiction, that M_i is an even block that is not symmetric. Since $n > 1$, there is an even 2-block M_{i+u} for some $u \neq 0$, and there must be a pair matching $(i, i+u)$. In each of five exhaustive cases,

R. Craigen is with Department of Mathematics, University of Manitoba, Winnipeg MB R3T 2N2, Canada.

J. Jedwab is with Department of Mathematics, Simon Fraser University, 8888 University Drive, Burnaby BC V5A 1S6, Canada.

Both authors are supported by NSERC grants.

Email: craigenr@cc.umanitoba.ca, jed@sfu.ca

2010 Mathematics Subject Classification 15B34 (primary), 94A55 (secondary)

this forces the existence of a further pair of even 2-blocks (M_j, M_{j+v}) for some j and v , where M_j is not symmetric, and there must be a pair matching $(j, j+v)$. Repeat this procedure. Since this procedure “cannot continue indefinitely,” we obtain a contradiction.

The following is a counterexample to this claimed procedure, using $n = 3$ and only the first of the five specified cases:

$$(M_0, M_1, M_2, M_3, M_4, M_5) = \left(\begin{bmatrix} + & + \\ + & + \end{bmatrix}, \begin{bmatrix} + & - \\ - & + \end{bmatrix}, \begin{bmatrix} - & - \\ - & - \end{bmatrix}, \begin{bmatrix} + & - \\ - & + \end{bmatrix}, \begin{bmatrix} - & - \\ - & - \end{bmatrix}, \begin{bmatrix} + & - \\ - & + \end{bmatrix} \right)$$

(writing $+$ for 1 and $-$ for -1). The even 2-blocks are M_0, M_2 , and M_4 , none of which is symmetric. Assign the matchings $(0, 2) \sim (2, 4)$ and $(0, 4) \sim (4, 2)$. Let $i = 0$ and $j = 2$, and follow the procedure of [3, p.8]. Since $(0, 2) \sim (2, 4)$, there must be a pair matching $(0, 4)$. Then, since $(0, 4) \sim (4, 2)$, there must be a pair matching $(0, 2)$. However $(0, 2)$ already has a matching pair $(2, 4)$, so the claimed contradiction does not arise.

References

- [1] R. Craigen and J. Jedwab. Comment on “The Hadamard circulant conjecture”. [arXiv:1111.3437v1](https://arxiv.org/abs/1111.3437v1) [math.CO].
- [2] B. Hurley, P. Hurley, and T. Hurley. The Hadamard circulant conjecture. *Bull. London Math. Soc.*, 2011. doi:10.1112/blms/bdq112.
- [3] B. Hurley, P. Hurley, and T. Hurley. The Hadamard circulant conjecture. [arXiv:1109.0748v1](https://arxiv.org/abs/1109.0748v1) [math.RA].