Comment on “The Hadamard circulant conjecture”

Robert Craigen Jonathan Jedwab

10 February 2011

Abstract

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

A *Hadamard matrix* of order m is an $m \times m$ matrix with entries in $\{1, -1\}$ satisfying $HH^T = mI_m$, where I_m is the $m \times m$ identity matrix. A *circulant* matrix is an $m \times m$ matrix for which each row except the first is a cyclic permutation of the previous row by one position to the right. The circulant Hadamard matrix conjecture [4, p.134] states that an $m \times m$ circulant Hadamard matrix exists only for $m = 1$ and $m = 4$. This conjecture has an equivalent formulation in terms of cyclic difference sets, and implies the Barker sequence conjecture [6] (see [2], [3], [5], for example, for background).

Hurley, Hurley and Hurley recently claimed [1] to have proved the circulant Hadamard matrix conjecture. We recap the necessary definitions from [1] and then present a counterexample to the claimed proof.

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 $i = -j$. Given a 2-block $D = \begin{bmatrix} i & j \\ j & i \end{bmatrix}$, define the 2-block $\widetilde{D} := \begin{bmatrix} j & i \\ i & j \end{bmatrix}$. A *4-block* is a matrix of the form $B = \begin{bmatrix} D_1 & D_2 \\ \widetilde{D_2} & D_1 \end{bmatrix}$, where D_1 and D_2 are 2-blocks. Given a 4-block $B = \begin{bmatrix} D_1 & D_2 \\ \widetilde{D_2} & D_1 \end{bmatrix}$, define the 4-block $\widetilde{B} := \begin{bmatrix} \widetilde{D_2} & D_1 \\ \widetilde{D_1} & \widetilde{D_2} \end{bmatrix}$. The proof of the main theorem of [1, p.9] asserts that the equation $B_i B_i^T = \widetilde{B_i} \left(\widetilde{B_i}\right)^T$, where B_i is a 4-block, implies that B_i consists of four even 2-blocks. The 4-block $B_i = \begin{bmatrix} + & - & + & + \\ - & + & + & + \\ + & + & + & - \\ + & + & - & + \end{bmatrix}$ (using $+$ for 1, and $-$ for -1) is a counterexample: this 4-block

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)

satisfies $B_iB_i^T = \widetilde{B_i}\left(\widetilde{B_i}\right)^T = 4I_4$, but consists of two even blocks and two odd blocks.

The error in [1] arises from a mistaken application of the following result. Let $B = \begin{bmatrix} D_1 & D_2 \\ \widetilde{D_2} & D_1 \end{bmatrix}$ and $C = \begin{bmatrix} D_3 & D_4 \\ \widetilde{D_4} & D_3 \end{bmatrix}$ be 4-blocks. Then Lemma 3.3 of [1] states that $BC = \widetilde{B}\widetilde{C}$ if and only if both D_1 and D_2 are even or both D_3 and D_4 are even. Application of this lemma with $B = B_i$ and $C = B_i^T$ would require the equation $B_iB_i^T = \widetilde{B_i}\widetilde{(B_i^T)}$ to hold, whereas what is established is that $B_iB_i^T = \widetilde{B_i}\left(\widetilde{B_i}\right)^T$ (which is just an identity); and in general $\widetilde{(B_i^T)} \neq \left(\widetilde{B_i}\right)^T$.

References

[1] B. Hurley, P. Hurley, and T. Hurley. The Hadamard circulant conjecture. *Bull. London Math. Soc.*, 2011. doi:10.1112/blms/bdq112.

[2] J. Jedwab. What can be used instead of a Barker sequence? *Contemp. Math.*, **461**:153–178, 2008.

[3] C. Lin and W.D. Wallis. On the circulant Hadamard matrix conjecture. In D. Jungnickel and S.A. Vanstone, editors, *Coding Theory, Design Theory, Group Theory*, pages 213–217. Wiley, New York, 1993.

[4] H.J. Ryser. *Combinatorial Mathematics.* Carus Mathematical Monographs No. 14. Mathematical Association of America, Washington, DC, 1963.

[5] B. Schmidt. *Characters and Cyclotomic Fields in Finite Geometry*, volume 1797 of *Lecture Notes in Mathematics.* Springer, Berlin, 2002.

[6] R. Turyn. Optimum codes study. Final Report. Contract AF19(604)-5473, Sylvania Electronic Systems, 29 January 1960.