EasyChair Preprint

№ 8250

Hadamard Conjecture Proof

Valerii Sopin

June 12, 2022

Hadamard Conjecture Proof

Valerii Sopin
email: VvS@myself.com

June 12, 2022

Abstract

The most important open question in the theory of Hadamard matrices is that of existence (the Hadamard conjecture). The generalization of Sylvester's construction proves that if H_n and H_m are Hadamard matrices of orders n and m, respectively, then $H_n \otimes H_m$ given by the Kronecker product is a Hadamard matrix of order nm. This result is used to produce Hadamard matrices of higher order once those of smaller orders are known.

Here we go in the opposite direction: we show how to construct a Hadamard matrix of order $4n$ from a Hadamard matrix of order $4nm$. The outcome gives the link to Number Theory with a way to prove the Hadamard conjecture, using Paley's work.

1 Introduction

A Hadamard matrix, named after French mathematician Jacques Hadamard [1], is a square matrix whose entries are either $+1$ or -1 and whose rows are mutually orthogonal. In combinatorial terms, it means that each pair of rows has matching entries in exactly half of their columns and mismatched entries in the remaining columns. It is a consequence of this definition that the corresponding properties hold for columns as well. A Hadamard matrix has maximal determinant among matrices with entries of absolute value less than or equal to 1 and so is an extremal solution of Hadamard's maximal determinant problem [1]. The last indicates that the order of a Hadamard matrix must be 1, 2, or a multiple of 4.

The Hadamard conjecture proposes that a Hadamard matrix of order $4k$ exists for every natural k. Many authors developed methods to construct Hadamard matrices (Sylvester's construction [2] and Paley's work [3] are the most famous). There are infinitely many orders of Hadamard matrices have been constructed. However, the conjecture has been open (the smallest order, for which the existence of a Hadamard matrix is in doubt, is currently $668 = 4 \cdot 167$).

It is apparent that if the rows and columns of a Hadamard matrix are permuted, the matrix remains Hadamard. It is also true that if any row or column is multiplied by -1, the Hadamard property is retained. Thus, it is always possible to arrange to have the first row and first column of a Hadamard matrix contain only $+1$ entries. A Hadamard matrix in this form is said to be normalized.

If H_{4k} is a normalized Hadamard matrix of order $4k$, then every row/column except the first has $2k$ minus ones and $2k$ plus ones. Further, k minus ones in any row/column overlap with k minus ones in each other row/column.

Hadamard matrices can be regarded as generalizations of the Walsh matrices (a non-standard branch of discrete Fourier analysis) and can almost directly be used as an error-correcting codes. Moreover, Hadamard matrices find applications in balanced repeated replication and in appraisal of the variance of a parameter estimator, see [4][5][6] and references therein.

In this paper we construct a Hadamard matrix of order $4n$ from a Hadamard matrix of order $4nm$ for any natural n and m. **The outcome** (along with known constructions of Hadamard matrices) **gives the resulting solution and the closure of the Hadamard conjecture** since it is left to show that for any prime number p there exists a natural number k that a Hadamard matrix of order $4pk$ can be constructed using known results.

Indeed, Paley's construction [3] produces a Hadamard matrix of order $q+1$ when q is any prime power that is congruent to 3 modulo 4 and a Hadamard matrix of order $2(q+1)$ when q is a prime power that is congruent to 1 modulo 4. So, the question about divisors of $q+1$ with prime q raises. But it can be reformulated as existence of a prime number of the form $4pk-1$ with fixed prime p and any natural k. The last amounts to Dirichlet's theorem on primes in arithmetic progressions.

It is worthy to mention that Hadamard matrices of order $4k^4$ exist for all odd k [7].

2 Reduction

There are at least three possible ways (the last one is the most evident). The implication $4nm \Rightarrow 4n$ guarantees that the chain survives.

Notice that a Hadamard matrix is symmetric if $H_{4k} = H_{4k}^t$ and is skew if $H_{4k} - I_{4k}$ is skew-symmetric, i.e. $H_{4k} + H_{4k}^t = 2I_{4k}$. Paley's first construction gives skew Hadamard matrices and the second construction gives symmetric ones [3].

For more constructions of Hadamard matrices check [8].

2.1 Pigeonhole principle

The pigeonhole principle states that if n items are put into m containers, with $n > m$, then at least one container must contain more than one item. In a more quantified version: for natural numbers k and m, if $n = km + 1$ objects are distributed among m sets, then the pigeonhole principle asserts that at least one of the sets will contain at least $k + 1$ objects.

2.2 Hadamard codes

Hadamard codes are obtained from an 4n-by-4n Hadamard matrix H [6]. In particular, the $8n$ codewords of the code are the rows of H and the rows of $-H$. To obtain a code over the alphabet $\{0, 1\}$, the mapping

$$x \longrightarrow (1 - x)/2$$

is applied to the matrix elements.

That the minimum distance of the code is $2n$ follows from the defining property of Hadamard matrices, namely that their rows are mutually orthogonal. This implies that two distinct rows of a Hadamard matrix differ in exactly $2n$ positions, and, since negation of a row does not affect orthogonality, that any row of H differs from any row of $-H$ in $2n$ positions as well, except when the rows correspond, in which case they differ in $4n$ positions. Thus, a Hadamard code is a $[4n, 2n, 2n]$ not-necessarily-linear code and it will correct any error pattern of weight $(n - 1)$, see Theorem 1 from [6].

It is needed to use the techniques of puncturing and shortening from coding theory.

2.3 Integer lattices

Let L be an integer lattice and S a set of lattice points in L. It is said that the set S is optimal if it minimises the number of rectangular sublattices of L (including degenerate ones) which contain an even number of points in S. The resolution of the Hadamard conjecture is equivalent to the determination of $|S|$ for an optimal set S in a $(4s - 1) \times (4s - 1)$ integer lattice L, see [9].

References

[1] Jacques Hadamard, *Résolution d'une question relative aux déterminants*, Bulletin des Sciences Mathématique, **17**, 1893, 240–246.

[2] James Joseph Sylvester, *Thoughts on inverse orthogonal matrices, simultaneous sign successions, and tessellated pavements in two or more colours, with applications to Newton's rule, ornamental tile-work, and the theory of numbers*, Philosophical Magazine, **34**, 1867, 461–475.

[3] Raymond Edward Alan Christopher Paley, *On orthogonal matrices*, Journal of Mathematics and Physics, **12**, 1933, 311–320.

[4] K. J. Horadam, *Hadamard Matrices and Their Application*, Princeton University Press, 2007.

[5] A. Hedayat and W. D. Wallis, *Hadamard Matrices and Their Applications*, The Annals of Statistics, **6**, 1978, 1184–1238.

[6] R.C. Bose and S.S. Shrikhande, *A note on a result in the theory of code construction*, Information and Control, **2** : 2, 1959, 183–194.

[7] Mikhail Muzychuk and Qing Xiang, *Symmetric Bush-type Hadamard matrices of order* $4m^4$ *exist for all odd* m, Proceedings of the American Mathematical Society, **134** : 8, 2006, 2197–2204.

[8] Jennifer Seberry and Mieko Yamada, *Hadamard Matrices: Constructions using Number Theory and Linear Algebra*, John Wiley and Sons, 2020.

[9] J. McCall and C.H.C. Little, *The Hadamard conjecture and integer lattices*, Journal of the Australian Mathematical Society (Series A), **43**, 1987, 257–267.