National University of Ireland, Galway
Ollscoil na hÉireann, Gaillimh

On Hadamard matrices from difference sets

Padraig Ó Catháin

Introduction

- A ± 1 matrix of order n which satisfies the equation $HH^T = nI_n$ is called a Hadamard matrix.
- Hadamard matrices are used in coding theory, statistics, combinatorial design theory, and many other fields of mathematics.
- Cocyclic Hadamard matrices are Hadamard matrices whose automorphism groups have a subgroup with an almost-regular action.
- Most known infinite families of Hadamard matrices come from difference sets.
- We use results on 2-transitive groups to describe the automorphism groups of these matrices, showing in particular that the matrices arising from twin prime power difference sets are not cocyclic.

Difference sets

Let G be a group of order v, and let $\mathcal{D}$ be a subset of G of cardinality k. We say that $\mathcal{D}$ is a (v, k, λ)-*difference set* if every non-identity element of G may be expressed in exactly λ ways as a quotient of elements of $\mathcal{D}$. Let $\chi_{\mathcal{D}}$ denote the characteristic function of $\mathcal{D}$. Then the *development* of $\mathcal{D}$ is the matrix

$$Dev(\mathcal{D}) = [\chi_{\mathcal{D}}(gh)]_{g,h\in G}.$$

We call a difference set with parameters $(4n-1, 2n-1, n-1)$ a *Hadamard difference set* as it gives rise to a Hadamard matrix in a natural way.

Lemma 1. *Let $\mathcal{D}$ be a $(4n-1, 2n-1, n-1)$-difference set. Define D to be $2\,\mathrm{Dev}\,(\mathcal{D}) - J$, and $\bar{1}$ to be the all 1s vector of length $4n-1$. Then*

$$H = \begin{pmatrix} 1 & \bar{1} \\ \bar{1}^{\top} & D \end{pmatrix}$$

is Hadamard. Furthermore, $\mathrm{PermAut}(H)$ *is isomorphic to* $\mathrm{Aut}(\mathcal{D})$.

Note that the automorphism group of a cocyclic Hadamard matrix, H, acts transitively on the rows of H, and that the automorphism group of D acts transitively on the rows of D.

Two-transitive groups

Let G be a group acting on a set X. We say that the action of G is 2-transitive if for any four distinct elements $w, x, y, z \in X$ there exists $g \in G$ such that

$$wg = y, \quad xg = z.$$

Lemma 2. *If H is a Hadamard matrix arising from a difference set, then* $\mathrm{Aut}(H)$ *is transitive if and only if it is 2-transitive.*

Now, deep results in group theory yield a complete classification of the finite 2-transitive groups. Furthermore a result of Ito states the following:

Theorem 3 (Ito). *Let $\Gamma \leq \mathrm{Aut}(H)$ be a doubly transitive permutation group acting on the set of rows of a Hadamard matrix, H. Then one of the following holds:*

- *$\Gamma \cong M_{12}$ and H is the unique Hadamard matrix of order 12.*
- *$PSL_2(p^k) \trianglelefteq \Gamma$, acting naturally on p^k+1 points, for $p^k \equiv 3 \mod 4$, $p^k \neq 3, 11$.*
- *$\Gamma \cong Sp_6(2)$, and H is of order 36.*
- *Γ contains a regular elementary abelian subgroup, and H is of order 2^n.*

A little elementary number theory

By twin prime powers we mean a pair of integers, q and $q+2$, both of which are prime powers. In this section, we prove the following:

Theorem 4. *The number $2^{2n}-1$ is a product of twin primes if and only if $n \in \{2, 3\}$.*

To this end, we will make use of a well known theorem of Zsigmondy.

Theorem 5 (Zsigmondy). *Let a, b and n be positive integers such that $(a, b) = 1$. Then there exists a prime p with the following properties:*

- *$p \mid a^n - b^n$*
- *$p \nmid a^k - b^k$ for all $k < n$.*

with the following exceptions: $a = 2, b = 1, n = 6$ and $a+b = 2^k, n = 2$.

Proof of Theorem 4: Assume $2^{2n}-1$ is a product of twin prime powers.

$$2^{2n} - 1 = (2^n+1)(2^n-1) = p_1^s p_2^r$$

Without loss of generality, $p_1^s = 2^n - 1$. There are two cases to consider: either $2^n \equiv 1 \mod 3$, or $2^n \equiv 2 \mod 3$.

In the first case, $p_1 = 3$. Then we apply Zsigmondy's theorem to the equation $2^n - 1 = 3^s$, to obtain $n = 2$ and $s = 1$.

In the second case, $p_2 = 3$, and we have $3^r - 1 = 2^n$. Zsigmondy's theorem gives us that $r = 1$ or $r = 2$. The first of these is a vacuous solution however, as it gives $p_1 = 1$. □

Twin prime power difference sets

Finally, we define the twin prime power difference sets and state our main theorem. Let q and $q+2$ be twin prime powers, let $4n-1 = q(q+2)$. Denote by F_q the Galois field of size q, and by χ the standard quadratic residue function. Then

$$\{(g, 0) \mid g \in F_q\} \bigcup \{(g, h) \mid g \in F_q, h \in F_{q+2}, \chi(g)\,\chi(h) = 1\}$$

is a $(4n-1, 2n-1, n-1)$-difference set in $(F_q, +) \times (F_{q+2}, +)$. We refer to such a difference set as a *TPP-difference set*.

Theorem 6. *Let H be a TPP-Hadamard matrix. Then H is cocyclic if and only if it is of order 16.*

Proof. Let H be a cocyclic TPP-Hadamard matrix of order $4n$. Then by Lemma 2, the automorphism group of H acts 2-transitively on the rows of H. Then by Ito's Theorem, we know that either $4n-1 = p^m$ or $n = 2^m$. We consider first the non affine case.

Ito's two sporadic 2-transitive actions are easily discarded: 11 is not a product of twin prime powers, and by construction the TPP-matrix of order 36 is not cocyclic, as it has an intransitive automorphism group. This leaves only the infinite family of matrices acted upon by $PSL_2(p^k)$. Recall that $PSL_2(p^k)$ has a unique 2-transitive action on p^k+1 points. These are ruled out by the following observation: suppose H is a TPP-Hadamard matrix, of order $q(q+2)+1$. Then

$$p^k = q(q+2).$$

The only solution to this equation in positive integers has $p = q = 2$, which is not a valid solution since $8 \neq 3 \mod 4$.

In the affine case, via Theorem 4, we have that the order of H is either 16 or 64. Construction of the matrices of these orders then shows that the one of order 16 is cocyclic, and is equivalent to the Sylvester matrix of that order, and that the one of order 64 is not. The required result follows. □

[1] T. Beth, D. Jungnickel, H. Lenz Design Theory, Vol. 1. Cambridge, 1999.

[2] P. Ó Catháin and M. Röder. The cocyclic Hadamard matrices of order at most 40. *Designs, Codes and Cryptography*, to appear.

[3] P. Ó Catháin and R. Stafford. On Twin prime power Hadamard matrices. *Cryptography and Communications: Discrete Structures, Boolean Functions and Sequences*, to appear.

School of Mathematics, Statistics and Applied Mathematics, National University of Ireland, Galway.