1973

A note on amicable Hadamard matrices

Jennifer Seberry
University of Wollongong, jennie@uow.edu.au

Publication Details
Jennifer Seberry Wallis, A note on amicable Hadamard matrices, Utilitas Mathematica, 3, (1973), 119-125.

A note on amicable Hadamard matrices

Abstract

The existence of Szekeres difference sets, X and Y, of size 2f with y E Y = -y E Y, where q = 4f + 1 is a prime power, q = 5 (mod 8) and q = p2 + 4, is demonstrated. This gives amicable Hadamard matrices of order 2(q + 1), and if 2q is also the order of a symmetric conference matrix, a regular symmetric Hadamard matrix of order $4q^2$ with constant diagonal.

Disciplines

Physical Sciences and Mathematics

Publication Details

Jennifer Seberry Wallis, A note on amicable Hadamard matrices, Utilitas Mathematica, 3, (1973), 119-125.

A NOTE ON AMICABLE HADAMARD MATRICES

Jennifer Wallis*

ABSTRACT. The existence of Szekeres difference sets, X and Y, of size $2f$ with $y \in Y \Rightarrow -y \in Y$, where $q = 4f + 1$ is a prime power, $q \equiv 5 \pmod 8$ and $q = p^2 + 4$, is demonstrated. This gives amicable Hadamard matrices of order $2(q + 1)$, and if $2q$ is also the order of a symmetric conference matrix, a regular symmetric Hadamard matrix of order $4q^2$ with constant diagonal.

Amicable Hadamard matrices are also constructed for orders $4(q + 1)$ where $q = 4f + 1 \equiv 5 \pmod 8$ is a prime power, $q = p^2 + 36$, by using $4 - \{4f + 1;\ 2f;\ 4f - 2\}$ supplementary difference sets $A, B = C = D$ with $a \in A \Rightarrow -a \notin A$, $b \in B \Rightarrow -b \in B$.

We assume the definition of such concepts as *Hadamard matrix, skew-Hadamard matrix, amicable Hadamard matrices, regular Hadamard matrix, symmetric conference matrix, supplementary difference sets* and *Szekeres difference sets* which may be found in [4] and the theory of *cyclotomy* a reference for which is [1].

LEMMA 1. *If* $q = 4f + 1$ (f *odd*) *is a prime power of the form* $q = p^2 + 4$, *then there exists* $2 - \{q = 4f + 1;\ 2f;\ 2f - 1\}$ *supplementary difference sets* A *and* B *such that* $a \in A \Rightarrow -a \notin A$ *and* $b \in B \Rightarrow -b \in B$ (*alternatively there exist Szekeres difference sets* A *and* B *of size* $2f$ *with* $b \in B \Rightarrow -b \in B$).

Proof. We proceed as in the proof of Szekeres-Whiteman theorem in [4; p. 323]. Let x be a generator of GF(q) and write

$$C_i = \{x^{4j+i} : 0 \le j \le f - 1\} \qquad i = 0,1,2,3.$$

---

* This paper was prepared while the author was a Postdoctoral Fellow in the Department of Statistics at the University of Waterloo.

UTILITAS MATHEMATICA, Vol. 3 (1973), pp. 119-125.

Choose

$$A = C_0 \cup C_1 \quad \text{and} \quad B = C_0 \cup C_2 \ .$$

Clearly $-1 \in C_2$ and $a \in A \Rightarrow -a \notin A$, $b \in B \Rightarrow -b \in B$.

We want to find the number N_k of solutions of $y - x = d$ with $x,y \in A$, $d \in C_k$: we use the notation of Storer [1]. Now

$$N_k = (-k,-k) + (1 - k, -k) + (-k, 1 - k) + (1 - k, 1 - k) \ .$$

The corresponding number $N_k{}^1$ of solutions of $y - x = d$, with $x, y \in B$, $d \in C_k$ is given by

$$N_k{}^1 = (-k,-k) + (2 - k, -k) + (-k, 2 - k) + (2 - k, 2 - k).$$

Clearly $N_k = N_{k+2}$ and $N_k{}^1 = N_{k+2}{}^1$ since $-1 \in C_2$. Using the array from Storer [1, p. 28] we see

$$N_0 = A + E + B + E,$$

$$N_0^1 = A + A + C + A,$$

$$N_1 = E + D + E + A,$$

$$N_1^1 = E + B + D + E.$$

Then using lemma 19 of page 48 of [1] we see

$$16(N_0 + N_0^1) = 16(4A + B + C + 2E) = 8q - 32 - 8t$$

$$16(N_1 + N_1^1) = 16(A + B + 2D + 4E) = 8q - 16 + 8t \ .$$

These expressions are equal for $t = -1$ that is (from lemma 19 of Storer) for $q = s^2 + 4$ where $s \equiv 1 \pmod 4$. If $p \equiv 1 \pmod 4$ put $s = p$ and if $p \equiv 3 \pmod p$ put $s = -p$ and we have $q = p^2 + 4$ of the statement of the lemma.

COROLLARY 2. *If* $q = 4f + 1 = p^2 + 4$ *is a prime power* (f *odd*) *there exist amicable Hadamard matrices of order* $2(q + 1)$.

Proof. Use theorem 2 of [3].

LEMMA 3. *If* $q = 4f + 1 = p^2 + 36$ *(f odd) is a prime power then there exist* $4 - \{4f + 1;\ 2f;\ 4f - 2\}$ *supplementary difference sets* A, B, C, D *with* $B = C = D$ *and such that* $a \in A \Rightarrow -a \notin A$, $b \in B \Rightarrow -b \in B$.

Proof. We use the notation of the proof of lemma 1 and choose

$$A = C_0 \cup C_1 \qquad B = C = D = C_1 \cup C_3 .$$

Then as before

$$N_k = (-k, -k) + (-k, 1 - k) + (1 - k, -k) + (1 - k, 1 - k) ,$$

$$N_k^1 = (1 - k, 1 - k) + (3 - k, 1 - k) + (1 - k, 3 - k) + \\ + (3 - k, 3 - k) .$$

Also, as before, $-1 \in C_2$, $N_k = N_{k+2}$, $N_k^1 = N_{k+2}^1$.

Then using Storer [1; p. 28 and p. 48] we have

$$N_0^1 = E + D + B + E,$$

$$N_1^1 = A + A + C + A,$$

so

$$16(N_0 + 3N_0^1) = 16(A + 4B + 3D + 8E) = 16q - 24 - 8t ,$$

$$16(N_1 + 3N_1^1) = 16(10A + 3C + D + 2E) = 16q - 72 + 8t .$$

Now these are equal for $t = 3$ and so from lemma 19 of Storer [1;p. 48] we have result for $q = s^2 + 4.9 = s^2 + 36$, $s \equiv 1 \pmod 4$, q is a prime power. As before we set $s = \pm p$ according as $p \equiv \pm 1 \pmod 4$ and we have $q = p^2 + 36$ as in the statement of the lemma.

LEMMA 4. *Suppose there exist* (1, -1)*-matrices* X, Y, Z, W *of order* q *satisfying*

$$X = -I + U,\ U^T = -U,\ Y^T = Y,\ Z^T = Z,\ W^T = W ,$$

$$XX^T + 3YY^T = 2ZZ^T + 2WW^T = 4(q + 1)I - 4J ,$$

and with $e = [1, \ldots, 1]$ *a* $1 \times q$ *matrix*

$$eX^T = eY^T = eZ^T = eW^T = -e,\ XY^T = YX^T \quad \textit{and} \quad ZW^T = WZ^T .$$

Then if

$$M = \begin{bmatrix} -1 & 1 & 1 & 1 & e & e & e & e \\ -1 & -1 & -1 & 1 & -e & e & -e & e \\ -1 & 1 & -1 & -1 & -e & e & e & -e \\ -1 & -1 & 1 & -1 & -e & -e & e & e \\ -e^T & e^T & e^T & e^T & X & Y & Y & Y \\ -e^T & -e^T & -e^T & e^T & -Y & X & -Y & Y \\ -e^T & e^T & -e^T & -e^T & -Y & Y & X & -Y \\ -e^T & -e^T & e^T & -e^T & -Y & -Y & Y & X \end{bmatrix}$$

$$N = \begin{bmatrix} 1 & 1 & 1 & 1 & e & e & e & e \\ 1 & -1 & -1 & 1 & e & -e & -e & e \\ 1 & -1 & 1 & -1 & e & -e & e & -e \\ 1 & 1 & -1 & -1 & e & e & -e & -e \\ e^T & e^T & e^T & e^T & Z & Z & W & W \\ e^T & -e^T & -e^T & e^T & Z & -Z & -W & W \\ e^T & -e^T & e^T & -e^T & W & -W & Z & -Z \\ e^T & e^T & -e^T & -e^T & W & W & -Z & -Z \end{bmatrix}$$

M *is a skew-Hadamard matrix and* N *is a symmetric Hadamard matrix of order* $4(q + 1)$. *Further, if*

$$XZ^T,\ XW^T,\ YZ^T,\ YW^T$$

are symmetric, M *and* N *are amicable Hadamard matrices.*

Proof. By straightforward verification.

COROLLARY 5. *If* $q = 4f + 1 = p^2 + 36$ (f *odd*) *is a prime power then there exist amicable Hadamard matrices of order* $4(q + 1)$.

Proof. With C_i as in the proof of lemma 1 define

$$A = C_0 \cup C_1,\ B = C_1 \cup C_3,\ D = C_0 \cup C_2 \ .$$

Choose X to be the type 1 (1, -1) incidence matrix of A and $Y = Z$ and W to be the type 2 (1, -1) incidence matrices of B and D respectively.

We have already observed that $a \in A \nRightarrow -a \notin A$, as X will be of the form $-I + U$ where $U^T = U$. Y, Z, W are all symmetric as they are type 2 (see [4; p. 288]). Also since A, B, D all have 2f elements

$$eX^T = eY^T = eZ^T = eW^T = -e \ .$$

$XY^T = YX^T$ follows from corollary 1.15 of [4]. B and D are the $2 - \{4f + 1; 2f; 2f - 1\}$ supplementary difference sets of lemma 1.8 of [4] and so using lemmas 1.21, 1.17 and 1.16 of [4] we have that

$$ZZ^T + WW^T = 4(2f + 1)I - 2J,\ ZW^T = WZ^T \ .$$

Further using lemmas 1.10 and 1.20 of [4] we have that the (1, -1) incidence matrices of A and B (using lemma 3) satisfy

$$AA^T + 3BB^T = 4(4f + 2)I - 4J \ .$$

Finally that

$$XZ^T,\ XW^T,\ YZ^T,\ YW^T$$

are all symmetric follows from corollary 1.15 of [4] and the fact that $Y = W$. Thus all the conditions of lemma 4 are satisfied and we have the corollary.

This gives amicable Hadamard matrices for the orders 248 and 496 for which they were not previously known.

This means there are amicable Hadamard matrices for the following orders:

I $\quad 2$;

II $\quad p^r + 1 \quad p^r$(prime power) $\equiv 3 \pmod 4$;

III	$2(q+1)$	q (prime power) $\equiv 1 \pmod 4$ and $2q+1$ a prime power;
IV	$2(q+1)$	q (prime power) $\equiv 5 \pmod 8$ $= p^2 + 4$;
V	$4(q+1)$	q (prime powers) $\equiv 5 \pmod 8$ $= p^2 + 36$;
VI	δ	where δ is the product of any of the above orders.

We also recall the following applications of amicable Hadamard matrices and Szekeres difference sets:

LEMMA 6. *If* m *and* m' *are the orders of amicable Hadamard matrices and there exists a skew-Hadamard matrix of order* $(m-1)m'/m$ *then there is a skew-Hadamard matrix of order* $m'(m'-1)(m-1)$.

LEMMA 7. [4; Theorem 5.15]. *Suppose there exist Szekeres difference sets,* X *and* Y, *of size* $2f$ *in an additive abelian group of order* $4f+1$ *with* $y \in Y \Rightarrow -y \in Y$. *Further suppose there is a symmetric conference matrix of order* $8f+2$. *Then there is a regular symmetric Hadamard matrix of order* $4(4f+1)^2$ *with constant diagonal.*

COROLLARY 8. *If* $q = 4f + 1$ (f *odd*) *is a prime power of the form* $q = p^2 + 4$ *and there is a symmetric conference matrix of order* $2q$ *there is a regular symmetric Hadamard matrix of order* $4q^2$ *with constant diagonal.*

Proof. Use lemmas 1 and 7.

COROLLARY 9. *If* q *(prime power)* $= p^2 + 4$, (p *odd*) *and* $2q-1$ *is a prime power there is a regular symmetric Hadamard matrix of order* $4q^2$ *with constant diagonal.*

The author wishes to thank Professor A. L. Whiteman for showing her that the restriction $p \equiv 1 \pmod 4$ was unnecessary in the results of this paper.

REFERENCES

[1] Thomas Storer, *Cyclotomy and Difference Sets*, Lectures in Advanced Mathematics, Markham, Chicago, 1967.

[2] G. Szekeres, *Cyclotomy and complementary difference sets*, Acta Arithmetica *18* (1971), 349-353.

[3] Jennifer Wallis, *Amicable Hadamard Matrices*, J. Combinatorial Theory (Ser. A.) *11* (1971), 296-298.

[4] W. D. Wallis, Anne Penfold Street and Jennifer Seberry Wallis, *Combinatorics: Room Squares, Sum-free Sets, Hadamard Matrices*, Lecture Notes in Mathematics Volume 292, Springer-Verlag, Berlin, Heidelberg, New York, 1972.

[5] Albert Leon Whiteman, *An infinite family of skew-Hadamard matrices*, Pacific J. Math. *38* (1971), 817-822.

University of Newcastle
New South Wales, 2308
Australia

Received September 25, 1972.