A Note on the Construction of $GH(4tq; EA(q))$ for $t = 1, 2$

Warwick de Launey
Cryptomathematics Research Group
Communications Division, ERL,
Defence Science and Technology Organisation
Melbourne, Australia 3004

Jeremy E. Dawson
Department of Defence
Melbourne, Australia 3000

Abstract

Let $GH(n; G)$ denote a generalised Hadamard matrix of order n over the group G, and let $EA(q)$ denote the elementary abelian group of prime power order q. We use a computer to investigate the applicability of a recently discovered general construction for $GH(4tq; EA(q))$ in the case $t = 2$. In particular, we prove that $GH(8p; Z_p)$ exist for all primes $p > 19$, and obtain $GH(8q; EA(q))$ for all prime powers q between 19 and 200 except 27. We also obtain a result on the number of "solutions" of a specific form, which suggests there are many inequivalent $GH(4q; EA(q))$. A consequence of our argument is a recasting of the Hadamard conjecture in terms of the behaviour of the discrete Fourier transform.

1 Preliminaries

Let q denote an odd prime power, p denote an odd prime, $EA(q)$ denote the elementary abelian group of order q, $GF[q]$ denote the Galois field of order q, and let χ denote the quadratic character on $GF[q]$; so $\chi(\alpha) = \alpha^{(q-1)/2}$.

Australasian Journal of Combinatorics 6(1992), pp.177-186

1.1 Definition: Let G be a finite group and $X = (x_{ij})$ be an $n \times n$ matrix over G such that each element appears $n/|G|$ times in each of the lists

$$x_{a1}x_{b1}^{-1}, x_{a2}x_{b2}^{-1}, \cdots, x_{an}x_{bn}^{-1}, \quad \text{and} \quad x_{1a}x_{1b}^{-1}, x_{2a}x_{2b}^{-1}, \cdots, x_{na}x_{nb}^{-1}.$$

Then X is a *generalised Hadamard matrix* $GH(n; G)$. □

We construct generalised Hadamard matrices of order $4tq$ for $t = 1, 2$. In particular, we prove the following theorem.

1.2 Theorem: *There exist* $GH(8p; Z_p)$ *for all odd primes* $p > 19$. □

Designs which can be directly derived from these designs include complete resolvable transversal designs, near complete transversal designs, group divisible designs, orthogonal arrays, large sets of mutually orthogonal F-squares, balanced incomplete block designs, extremal equidistant codes.

2 A Construction for $GH(4tq; EA(q))$

Generalising work by Jungnickel [4] and Street [5], Dawson [1] constructed $GH(4q; EA(q))$ of the form (H_{ij}) where each matrix H_{ij} is a $GH(q; EA(q))$ and each of the following submatrices are $GH(2q; EA(q))$ matrices:

$$\begin{pmatrix} H_{sv} & H_{sw} \\ H_{tv} & H_{tw} \end{pmatrix},$$

for all

$$(s,t;v,w) \in S = \left\{ \begin{array}{llll} (1,2;1,2), & (1,3;1,3), & (1,4;1,4), & (3,4;3,4), \\ (2,4;2,4), & (2,3;2,3), & (1,2;3,4), & (1,3;2,4), \\ (1,4;2,3), & (3,4;1,2), & (2,4;1,3), & (2,3;1,4) \end{array} \right\}.$$

Specifically, Dawson set

$$H_{ij} = (h_{xz}^{ij} = \alpha_{ij}z^2 + 2\beta_{ij}xz + \gamma_{ij}x^2)_{x,z \in GF[q]}, \tag{2.1}$$

and solved the following set of equations over $GF[q]$:

$$\frac{\alpha_{sv}-\alpha_{tv}}{\beta_{sv}.\beta_{tv}} = \frac{\alpha_{sw}-\alpha_{tw}}{\beta_{sw}.\beta_{tw}}, \tag{2.2}$$

$$\frac{\gamma_{sv}-\gamma_{sw}}{\beta_{sv}.\beta_{sw}} = \frac{\gamma_{tv}-\gamma_{tw}}{\beta_{tv}.\beta_{tw}}, \tag{2.3}$$

$$\frac{\alpha_{sv}-\alpha_{tv}}{\beta_{sv}.\beta_{tv}}.\frac{\gamma_{sv}-\gamma_{sw}}{\beta_{sv}.\beta_{sw}} = \frac{\beta_{sv}\beta_{tw}-\beta_{sw}\beta_{tv}}{\beta_{sv}\beta_{sw}\beta_{tv}\beta_{tw}}, \tag{2.4}$$

$$\chi(\beta_{sv}\beta_{sw}\beta_{tv}\beta_{tw}) = -1, \tag{2.5}$$

where $(s,t;v,w) \in S$, under the constraint that no denominator or numerator is zero. The possibility of extending this approach to obtain $GH(2sq;EA(q))$ of the form (H_{ij}), where

$$H_{ij} = (\alpha_{ij}x^2 + \beta_{ij}xy + \gamma_{ij}y^2)_{x,y\in GF(q)}, \tag{2.6}$$

was discussed in [2]. (Any such attempt would require the solution of the equations over a set S' containing at least $(2s-1)s^2$ 4-tuples.) It was noted that equation (2.5) would then force the matrix

$$B = (\chi(\beta_{ij}))$$

to be a Hadamard matrix; so that $s = 2t$ must be even. In [2], the following conjecture was made.

2.1 Conjecture: *There exists a $GH(4tq;EA(q))$ for all prime powers q and integers $t > 0$.* □

Recently [3], the following asymptotic result was proved.

2.2 Theorem: *Suppose there exists an Hadamard matrix of order $k \geq 8$. Then for all odd prime powers $q \geq \left((k-2)2^{k-2} - k(k-1)/2 + 3\right)^2$ there exists a $GH(kq;EA(q))$.* □

3 Two General Solutions to the First Three of Dawson's Equations

A crucial step in proving Theorem 2.2 was the discovery of the following two general solutions to the first three of Dawson's equations.

3.1 First solution: *Let $f_1, f_2, \cdots, f_t, g_1, g_2, \cdots, g_t$ be elements of $GF(q)$ such that, for all $i, j = 1, 2, \cdots, t$, $f_i g_j \neq 1$ and, for $i \neq j$, $f_i \neq f_j$ and $g_i \neq g_j$. Set*

$$\beta_{ij} = (1 - f_i g_j)^{-1}, \quad \alpha_{ij} = f_i \beta_{ij}, \quad \text{and} \quad \gamma_{ij} = g_j \beta_{ij}.$$

These satisfy equations (2.2) - (2.4), and, if the matrix

$$B_1 = (\chi(1 - f_i g_j)) \tag{3.7}$$

is an Hadamard matrix, they also satisfy equation (2.5). □

3.2 Second solution: *Let $f_1, f_2, \cdots, f_t, g_1, g_2, \cdots, g_t$ be distinct elements of $GF(q)$ such that, for all $i = 1, 2, \cdots, t$, $f_i \neq 0$. Set*

$$\beta_{ij} = (f_i - g_j)^{-1}, \quad \alpha_{ij} = \beta_{ij}, \quad \text{and} \quad \gamma_{ij} = f_i^{-1} g_j \beta_{ij}.$$

These satisfy equations (2.2) - (2.4), and, if the matrix

$$B_2 = (\chi(f_i - g_j)) \tag{3.8}$$

is an Hadamard matrix, they also satisfy equation (2.5). □

The generalised Hadamard matrices presented in the next section are the result of computer searches for Hadamard matrices of one of the forms (3.7) and (3.8).

4 Results for $GH(8q; EA(q))$

The second form allows the problem of finding a solution to be transformed into a problem about the distribution of the quadratic character of the field $GF(q)$. When $q = p$ is a prime, the Legendre sequence $\{\chi(i)\}_{i=1,2,\cdots,p-1}$ becomes important. In particular, if it is possible to find each of the rows of an 8×8 Hadamard matrix embedded as contiguous subsequences of length 8 in the Legendre sequence of p, then there is a solution of the second form for p. Let us say an 8-tuple is exceptional for a prime p if neither itself nor its negation appears in the Legendre sequence of p.

The asymptotic result Theorem 2.2 gives $GH(8q; EA(q))$ for any odd prime power $q \geq 128,881$. Matrices given by this result are all of the second form. However, using a computer we found that the largest prime for which there is an exceptional 8-tuple is 1621. So for primes p greater than 1621 every 8×8 $(1, -1)$-matrix is

P.	Poly.	Gen.	Exp. for $g_2 \cdots g_8$							Exp. for $f_2 \cdots f_8$						
25	1,3	1,2	0	1	4	7	13	15	17	2	4	1	10	15	22	21
49	1,4	1,1	0	1	2	3	4	37	45	30	31	34	35	25	4	22
81	1,2,1,2,1	1,1	0	1	2	3	4	8	12	39	40	43	73	11	51	47
121	1,9	1,2	0	1	2	3	4	5	42	94	48	49	54	8	56	10
125	1,3,1,2	1,0	0	1	2	3	4	7	10	98	34	2	36	65	87	58
169	1,11	1,2	0	1	2	3	4	5	8	69	70	138	65	37	95	9

Table 1: Solutions of the first form for prime powers $25 \leq q \leq 200$

equivalent to a matrix which can be written in the second form over $GF(p)$. Therefore, for all primes $p \geq 1621$, there is a $GH(8p; EA(p))$.

Moreover, we found that for primes p where $1000 \leq p \leq 130,000$ the first 1300 terms of the Legendre sequence contained ϵ or $-\epsilon$ for all but one or two 8-tuples ϵ. Indeed, we found that generally solutions of the second kind with $g_i = i$ $(i = 0, \cdots, 7)$ could be found by examining no more than the first 200 bits in the Legendre sequence. The largest prime for which this is not possible is 139. The next largest is 197. So finding solutions could be done very quickly.

More exhaustive tests yielded solutions of the first form for all prime powers q between 16 and 200 inclusive, except 17, 19 and 27. All but the design with $p = 23$ are tabulated in Tables 1 and 2. To obtain a $GH(8.23; Z_{23})$ put $g_1, \cdots g_8, f_1, \cdots f_8$ equal to $0, 1, 2, 3, 4, 7, 10, 12, 4, 9, 11, 13, 14, 15, 21, 22$, respectively. Complete computer searches showed there is no solution of either form for $q = 17, 19$ and 27.

4.1 Notes on Tables 1 and 2:

(i) The first entry in each row is the prime or prime power.

(ii) In Table 1, the second entry is the coefficients of the polynomial used to define the extension field.

(iii) The next is a generator ν for the multiplicative group of the field.

(iv) The final twelve entries are the powers to which ν is raised to give $g_2, \cdots g_8$, $f_2, \cdots f_8$.

(v) The quantities f_1 and g_1 are zero.

□

Prime	Gen.	Exp. for $g_2 \cdots g_8$							Exp. for $f_2 \cdots f_8$						
29	2	0	1	2	3	8	9	22	15	16	1	7	8	9	10
31	3	0	1	6	9	17	20	27	5	17	22	25	28	1	7
37	2	0	1	2	5	9	18	28	22	23	9	20	12	14	26
41	6	0	1	2	3	5	6	28	28	19	1	2	3	5	11
43	3	0	1	2	5	9	17	21	35	31	16	15	19	7	29
47	5	0	1	2	5	8	24	26	42	9	24	27	31	18	32
53	2	0	1	2	3	4	31	34	2	3	8	24	15	26	27
59	2	0	1	2	3	5	6	31	20	38	54	8	33	45	15
61	2	0	1	2	3	6	29	55	49	40	43	3	51	52	53
67	2	0	1	2	3	4	6	41	1	24	27	31	32	54	55
71	7	0	1	2	3	5	28	29	28	47	64	22	10	4	27
73	5	0	1	2	3	4	5	6	29	9	10	11	12	13	14
79	3	0	1	2	3	4	12	50	23	60	61	62	41	42	22
83	2	0	1	2	3	4	5	16	33	34	35	16	4	5	6
89	3	0	1	2	3	6	8	26	40	41	63	49	21	24	55
97	5	0	1	2	3	4	5	20	73	35	14	69	70	71	20
101	2	0	1	2	3	4	5	17	42	64	76	4	10	6	34
103	5	0	1	2	3	4	6	41	57	3	6	10	43	38	29
107	2	0	1	2	3	4	5	6	22	23	37	57	71	28	73
109	6	0	1	2	3	4	8	12	91	95	23	47	63	86	87
113	3	0	1	2	3	4	5	6	74	92	50	51	52	53	73
127	3	0	1	2	3	4	5	103	84	53	73	74	43	31	45
131	2	0	1	2	3	4	9	14	51	118	15	58	59	81	33
137	3	0	1	2	3	4	6	86	45	46	47	84	17	52	103
139	2	0	1	2	3	4	5	24	128	101	25	103	117	93	94
149	2	0	1	2	3	4	5	8	50	21	44	29	17	48	25
151	6	0	1	2	3	4	6	11	5	95	75	20	9	23	101
157	5	0	1	2	3	4	6	7	148	30	33	93	77	96	53
163	2	0	1	2	3	4	6	9	33	7	10	11	63	42	115
167	5	0	1	2	3	4	5	7	3	133	90	85	92	105	81
173	2	0	1	2	3	4	5	28	65	142	96	43	56	103	64
179	2	0	1	2	3	4	7	11	94	61	42	136	26	27	28
181	2	0	1	2	3	4	5	9	63	1	2	83	40	61	114
191	19	0	1	2	3	4	5	22	19	20	51	52	113	17	18
193	5	0	1	2	3	4	5	6	95	127	73	74	104	93	94
197	2	0	1	2	3	4	5	6	11	54	126	127	128	9	10

Table 2: Solutions of the first form for primes $23 < p < 200$

5 Results for $GH(4q; EA(q))$

In this section, we prove the following result.

5.1 Theorem: *For $t = 2$ and odd prime powers q the number of solutions of the second form is $O(q^8)$. Indeed, let $M(4, q)$ denote the number of the solutions of the second form; then, for any $\epsilon > 0$ and sufficiently large odd prime powers q,*

$$\frac{M(4,q)}{q^8} > 2^{-11} - \epsilon.$$

□

The proof relies on the following lemma which will be proved later.

5.2 Lemma: (Four Rows Lemma) *Any $4 \times n$ $(1, -1)$-matrix whose rows are pairwise orthogonal contains at least $2^{-11}n^4$ distinct 4×4 submatrices which are Hadamard.* □

Proof of Theorem 5.1. Pick any four distinct elements a, b, c, d of $GF(q)$. For $y \neq a, b, c, d$, put

$$L = \begin{pmatrix} \chi(y-a) \\ \chi(y-b) \\ \chi(y-c) \\ \chi(y-d) \end{pmatrix},$$

and

$$A_u = \begin{pmatrix} u & u & \chi(b-a) & \chi(c-a) & \chi(d-a) \\ u & \chi(a-b) & u & \chi(c-b) & \chi(d-b) \\ u & \chi(a-c) & \chi(b-c) & u & \chi(d-c) \\ u & \chi(a-d) & \chi(b-d) & \chi(c-d) & u \end{pmatrix}.$$

The number of solutions of the second form where the sequence g_0, g_1, g_2, g_3 equals the sequence a, b, c, d is the number of 4×4 submatrices of L which are Hadamard. The rows of the following $4 \times 2(q+1)$ $(1, -1)$ matrix are orthogonal.

$$\begin{pmatrix} A_1 & A_{-1} & L & -L \end{pmatrix}.$$

Hence it contains at least $2^{-11}(2(q+1))^4$ submatrices which are Hadamard. Moreover, the number of these submatrices not containing one of the first 8 columns is at least

$$a = 2^{-11}(2(q+1))^4 - \begin{pmatrix} 2(q+1) \\ 4 \end{pmatrix} + \begin{pmatrix} 2q-8 \\ 4 \end{pmatrix}.$$

Hence L contains at least $2^{-4}a$ Hadamard matrices of order 4. □

6 An Hadamard Transform Pair

In this section we discuss a pair of integer vectors which are of combinatorial interest and which are related by the Hadamard Transform. We use this pair to prove Lemma 5.2.

Let k be a positive integer, and let V^k be the vector space of k-tuples over $GF[2]$. Let $X = (x_{ij})$ be a $k \times n$ $(0,1)$-matrix, and let X^* denote the related $(1,-1)$-matrix $((-1)^{x_{ij}})$.

We now introduce the transform pair. Let $c(v)$ be the *number of columns of X which is equal to v*, and set $C(X)$ equal to the 2^k-dimensional vector $(c(v))$. To define the other vector we need the following definition.

6.1 Definition: Let $u \in V^k$. The *uth generalised inner product of X^** is the sum

$$p(u) = \frac{1}{2^k} \sum_{j=1}^{n} \left(\prod_{i=1}^{k} (-1)^{x_{ij} u_i} \right).$$

□

Now let $P(X)$ be the 2^k-dimensional vector $(p(u))$ $(u \in V^k)$. We observe that

6.2 Theorem: *Let $H = ((-1)^{u \cdot v})_{u,v \in V^k}$ be the Sylvester Hadamard matrix of order 2^k. Then for any $k \times n$ $(0,1)$-matrix,*

$$P(X) = H\ C(X).$$

Proof. Observe that

$$p(u) = \frac{1}{2^k} \sum_{v \in V^k} c(v)(-1)^{u \cdot v}.$$

□

7 Proof of the Four Orthogonal Rows Lemma

We now use Theorem 6.2 to prove the four rows lemma.

Proof of Lemma 5.2. Let X^* satisfy the hypothesis of the lemma. Consider

$$Y^* = \begin{pmatrix} X^* & -X^* \end{pmatrix}.$$

Note the number of 4×4 Hadamard matrices in X^* is 2^{-4} $\times$ the number of 4×4 Hadamard matrices in Y^*. Observe that

$$P(Y^*) = (2n, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2x),$$

where

$$x = \sum_{j=1}^{n} \prod_{i=0}^{4} x_{ij}.$$

Hence

$$\begin{aligned} C(Y) = \ & \tfrac{1}{8}(n+x, n-x, n-x, n+x, n-x, n+x, n+x, n-x \\ & , n-x, n+x, n+x, n-x, n+x, n-x, n-x, n+x). \end{aligned}$$

Now note that any four columns will comprise an order 4 Hadamard matrix if and only if they all contain an even number of ones or they all contain an odd number of ones. It follows that Y^* contains precisely

$$\left(\frac{1}{4}\right)^4 \left((n+x)^4 + (n-x)^4\right)$$

Hadamard matrices. This quantity is minimised when $x = 0$, and then its value is $2^{-7}n^4$. □

8 A Comment on the Hadamard Conjecture

It is conjectured that there is an Hadamard matrix of order $4t$ for all integers $t > 0$. Theorem 6.2 transforms this conjecture into a conjecture about the $(4t-1)$-dimensional Hadamard transform. Each Hadamard matrix of order $4t$ corresponds to an integer vector C whose transform P has its "impulse" and "doublet" components equal to zero and its "null" component equal to $4t$. The Hadamard transform has a number of striking algebraic properties which may provide a way of proving such integer vectors, and hence their corresponding Hadamard matrices, exist

It is well known that a Hadamard matrix corresponds to a non-negative integer solution of $4t(4t-1)/2$ linear constraints in 2^{4t-1} unknowns. Theorem 6.2 gives a succinct formulation of these linear constraints. Moreover, the theorem might be useful in classifying Hadamard matrices of the same order.

References

[1] J. Dawson. A construction for the generalised Hadamard matrices $GH(4q; EA(q))$. *Journal of Statistical Planning and Inference*, 11:103–110, 1985.

[2] W. de Launey. A survey of generalised Hadamard matrices and difference matrices with large r. *Utilitas Mathematica*, 30:5–29, 1986.

[3] W. de Launey and J. Dawson. An asymptotic result on the existence of generalised Hadamard matrices. *J. Comb. Th. Ser. A.* To appear.

[4] D. Jungnickel. On difference matrices, resolvable TDs and generalised Hadamard matrices. *Math. Z.*, 167:49–60, 1979.

[5] D. J. Street. Generalised Hadamard matrices, orthogonal arrays and F-squares. *Ars Combinatoria*, 3:131–141, 1979.

(Received 2/9/91)