CERTAIN HADAMARD DESIGNS

P. KESAVA MENON

1. The object of this paper is to construct Hadamard designs for the parameters

$$(1.1)\qquad v = 4m^2 - 1, \quad k = 2m^2 - 1, \quad \lambda = m^2 - 1, \quad n = m^2$$

where both $2m+1$ and $2m-1$ are prime powers.

2. Let $GF(p^l)$ be the Galois field of p^l elements and let x be a primitive element of the field. We shall denote the additive group of the field by F, the sets containing the odd and even powers of x by C_o, C_e respectively, and the set consisting of the single element o by C so that

$$(2.1)\qquad F = C + C_o + C_e.$$

If A, B are two aggregates of elements of F we shall denote by AB the aggregate formed by adding each element of A to every element of B. We shall also denote the aggregate obtained by taking A a times by $a\,A$. Then we have the following

LEMMA 1. *If* $p^l \equiv 1 \pmod 4$, *then*

$$(2.2)\qquad \begin{aligned} C_oC_e &= \frac{p^l - 1}{4}(C_o + C_e), \\ C_o^2 &= \frac{p^l - 1}{2}C + \frac{p^l - 5}{4}C_o + \frac{p^l - 1}{4}C_e, \\ C_e^2 &= \frac{p^l - 1}{2}C + \frac{p^l - 1}{4}C_o + \frac{p^l - 5}{4}C_e. \end{aligned}$$

PROOF. The aggregate C_oC_e consists of the elements

$$x^{2r-1} + x^{2s} \qquad (r, s = 1, 2, \cdots, (p-1)/2).$$

If $x^k = x^{2r-1} + x^{2s}$ then $x^{k+i} = x^{2r-1+i} + x^{2s+i}$ and one of $2r-1+i$, $2s+i$ is even and the other odd for all i. It follows that all elements x^k have the same number of representations as the sum of an odd power and an even power of x. Moreover, since $x^{(p^l-1)2} = -1$, and $(p^l-1)/2$ is even by hypothesis, -1 belongs to C_e and hence the negative of

Received by the editors June 19, 1961.

every element of C_e belongs to C_e so that C_oC_e does not contain the element o. It follows that

$$C_oC_e = a(C_o + C_e),$$

where a denotes the number of times each power of x occurs in C_oC_e. Equating the number of terms on either side we readily get

$$a = \frac{p^l - 1}{4}$$

so that

$$C_oC_e = \frac{p^l - 1}{4}(C_o + C_e). \tag{2.3}$$

Let us now observe that

$$C_oF = C_eF = \frac{p^l - 1}{2}F. \tag{2.4}$$

Subtracting (2.3) from (2.4) we get

$$\begin{aligned} C_o^2 + C_o &= \frac{p^l - 1}{2}C + \frac{p^l - 1}{4}(C_o + C_e) \\ &= C_e^2 + C_e, \end{aligned}$$

which completes the proof of the lemma.

LEMMA 2. *If* $p^l \equiv -1 \pmod 4$, *then*

$$\begin{aligned} C_oC_e &= \frac{p^l - 1}{2}C + \frac{p^l - 3}{4}(C_o + C_e), \\ C_o^2 &= \frac{p^l - 3}{4}C_o + \frac{p^l + 1}{4}C_e, \\ C_e^2 &= \frac{p^l + 1}{4}C_o + \frac{p^l - 3}{4}C_e. \end{aligned} \tag{2.5}$$

PROOF. The proof is exactly as in Lemma 1 except that in this case -1 is in C_o so that C_o consists of the negative of the elements of C_e and hence

$$C_oC_e = \frac{p^l - 1}{2}C + a(C_o + C_e)$$

where a is determined by equating the number of terms on either side.

3. We are now in a position to construct the designs in question, or equivalently to construct difference sets with the parameters (1.1).

THEOREM 1. *Let* $2m+1=p^r$, $2m-1=q^s$ *where* p, q *are primes. Let* F_p, F_q *be the additive groups of the Galois fields* $GF(p^r)$, $GF(q^s)$ *respectively and let* $G=(F_p, F_q)$ *be the direct-product of* F_p, F_q. *Let* C_p, $C_{p,o}$, $C_{p,e}$; C_q, $C_{q,o}$, $C_{q,e}$ *denote the sets consisting of the zero element only, the odd powers of the primitive element and the even powers of the primitive element respectively of* F_p; F_q. *Then the set* S *consisting of the pairs*

$$(C_p + C_{p,o}, C_{q,o}), \quad (C_p + C_{p,e}, C_{q,e}), \quad (C_p, C_q)$$

is a difference set in G.

PROOF. Let us write

$$\begin{aligned} A &= (C_p + C_{p,o}, C_{q,o}), \\ B &= (C_p + C_{p,e}, C_{q,e}), \\ C &= (C_p, C_q), \end{aligned}$$

so that

$$S = A + B + C.$$

We shall consider the two cases $p^r \equiv \pm 1 \pmod 4$ separately.

CASE (i). Let $p^r \equiv 1 \pmod 4$. Then $q^s = p^r - 2 \equiv -1 \pmod 4$. Hence

$$\begin{aligned} AA^{-1} &= (C_p + C_{p,o}, C_{q,o})(C_p + C_{p,o}, C_{q,e}) \\ &= ((C_p + C_{p,o})^2, C_{q,o}C_{q,e}), \\ BB^{-1} &= (C_p + C_{p,e}, C_{q,e})(C_p + C_{p,e}, C_{q,o}) \\ &= ((C_p + C_{p,e})^2, C_{q,o}C_{q,e}), \\ AB^{-1} &= (C_p + C_{p,o}, C_{q,o})(C_p + C_{p,e}, C_{q,o}) \\ &= ((C_p + C_{p,o})(C_p + C_{p,e}), C_{q,o}^2), \\ BA^{-1} &= (C_p + C_{p,e}, C_{q,e})(C_p + C_{p,o}, C_{q,e}) \\ &= ((C_p + C_{p,e})(C_p + C_{p,o}), C_{q,e}^2). \end{aligned}$$

Hence

$$\begin{aligned} SS^{-1} = {} & ((C_p + C_{p,o})^2 + (C_p + C_{p,e})^2, C_{q,o}C_{q,e}) \\ & + ((C_p + C_{p,o})(C_p + C_{p,e}), C_{q,o}^2 + C_{q,e}^2) \\ & + A + B + A^{-1} + B^{-1} + C. \end{aligned}$$

Since $p^r \equiv 1 \pmod 4$ we have, by Lemma 1,

$$
\begin{aligned}
&(C_p + C_{p,o})^2 + (C_p + C_{p,e})^2 \\
&\quad = 2(C_p + C_{p,o} + C_{p,e}) + C_{p,o}^2 + C_{p,e}^2 \\
&\quad = 2F_p + (p^r - 1)C_p + \frac{p^r - 3}{2}(C_{p,o} + C_{p,e}) \\
&\quad = \left(\frac{p^r + 1}{2}\right)(C_p + F_p) = (m + 1)(C_p + F_p)
\end{aligned}
$$

and

$$
\begin{aligned}
&(C_p + C_{p,o})(C_p + C_{p,e}) \\
&\quad = C_p + C_{p,o} + C_{p,e} + C_{p,o}C_{p,e} \\
&\quad = \left(\frac{p^r + 3}{4}\right)F_p - \left(\frac{p^r - 1}{4}\right)C_p = \frac{(m+2)}{2}F_p - \frac{m}{2}C_p
\end{aligned}
$$

and since $q^s \equiv -1 \pmod 4$ we have, by Lemma 2,

$$
\begin{aligned}
C_{q,o}C_{q,e} &= \left(\frac{q^s - 1}{2}\right)C + \left(\frac{q^s - 3}{4}\right)(C_{q,o} + C_{q,e}) \\
&= \left(\frac{q^s + 1}{4}\right)C + \left(\frac{q^s - 3}{4}\right)F_q = \frac{m}{2}C_q + \frac{m-2}{2}F_q
\end{aligned}
$$

and

$$
\begin{aligned}
C_{q,o}^2 + C_{q,e}^2 &= \left(\frac{q^s - 1}{2}\right)(C_{q,o} + C_{q,e}) \\
&= \left(\frac{q^s - 1}{2}\right)(F_q - C_q) = (m - 1)(F_q - C_q).
\end{aligned}
$$

Moreover,

$$
\begin{aligned}
A + A^{-1} &= (C_p + C_{p,o}, C_{q,o}) + (C_p + C_{p,o}, C_{q,e}) \\
&= (C_p + C_{p,o}, C_{q,o} + C_{q,e}), \\
B + B^{-1} &= (C_p + C_{p,e}, C_{q,e}) + (C_p + C_{p,e}, C_{q,o}) \\
&\quad + (C_p + C_{p,e}, C_{q,o} + C_{q,e}),
\end{aligned}
$$

so that

$$
A + A^{-1} + B + B^{-1} = (C_p + F_p, F_q - C_q).
$$

Hence we have

$$SS^{-1} = \left((m+1)(C_p + F_p), \frac{m}{2} C_q + \frac{m-2}{2} F_q\right)$$

$$+ \left(\frac{(m+2)}{2} F - \frac{m}{2} C_p, (m-1)(F_q - C_q)\right)$$

$$+ (C_p + F_p, F_q - C_q) + (C_p, C_q)$$

$$= \left\{\frac{m(m+1)}{2} + \frac{m(m-1)}{2}\right\} (C_p, C_q)$$

$$+ \left\{\frac{(m+1)(m-2)}{2} + \frac{(m+2)(m-1)}{2} + 1\right\} (F_p, F_q)$$

$$= m^2(C_p, C_q) + (m^2 - 1)G,$$

which proves that S is a difference set in G. Its parameters are easily seen to be

$$v = 4m^2 - 1, \quad k = 2m^2 - 1, \quad \lambda = m^2 - 1, \quad n = m^2.$$

CASE (ii). Let $p^r \equiv -1 \pmod 4$, $q^s = p^r - 2 \equiv 1 \pmod 4$.
In this case

$$\begin{aligned}
AA^{-1} &= (C_p + C_{p,o}, C_{q,o})(C_p + C_{p,e}, C_{q,o}) \\
&= (C_p + C_{p,o})(C_p + C_{p,e}), C_{q,o}^2), \\
BB^{-1} &= (C_p + C_{p,e}, C_{q,e})(C_p + C_{p,o}, C_{q,e}) \\
&= ((C_p + C_{p,e})(C_p + C_{p,o}), C_{q,e}^2), \\
AB^{-1} &= (C_p + C_{p,o}, C_{q,o})(C_p + C_{p,o}, C_{q,e}) \\
&= ((C_p + C_{p,o})^2, C_{q,o}C_{q,e}), \\
A^{-1}B &= (C_p + C_{p,e}, C_{q,o})(C_p + C_{p,e}, C_{q,e}) \\
&= ((C_p + C_{p,e})^2 C_{q,o}C_{q,e}), \\
A + A^{-1} &= (C_p + C_{p,o}, C_{q,o}) + (C_p + C_{p,e}, C_{q,o}) \\
&= (C_p + F_p, C_{q,o}), \\
B + B^{-1} &= (C_p + C_{p,e}, C_{q,e}) + (C_p + C_{p,o}, C_{q,e}) \\
&= (C_p + F_p, C_{q,e}).
\end{aligned}$$

Hence we have

$$\begin{aligned}
SS^{-1} = {} & ((C_p + C_{p,o})(C_p + C_{p,e}), C_{q,o}^2 + C_{q,e}^2) \\
& + ((C_p + C_{p,o})^2 + (C_p + C_{p,e})^2, C_{q,o}C_{q,e}) \\
& + (C_p + F_p, F_q - C_q) + (C_p, C_q).
\end{aligned}$$

But, by Lemma 1,

$$C_{q,o}^2 + C_{q,e}^2 = (q^s - 1)C_q + \frac{q^s - 3}{2}(C_{q,o} + C_{q,e})$$

$$= \frac{(q^s + 1)}{2} C_q + \frac{q^s - 3}{2} F_q = mC_q + (m - 2)F_q,$$

$$C_{q,o}C_{q,e} = \frac{q^s - 1}{4}(C_{q,o} + C_{q,e}) = \frac{m - 1}{2}(F_q + C_q)$$

and, by Lemma 2,

$$(C_p + C_{p,o})(C_p + C_{p,e})$$
$$= C_p + C_{p,o} + C_{p,e} + C_{p,o}C_{p,e}$$
$$= F_p + \frac{p^r - 1}{2} C_p + \frac{p^r - 3}{4}(C_{p,o} + C_{p,e})$$
$$= \frac{p^r + 1}{4}(F_p + C_p) = \frac{m + 1}{2}(F_p - C_p),$$

$$(C_p + C_{p,o})^2 + (C_p + C_{p,e})^2$$
$$= 2(C_p + C_{p,o} + C_{p,e}) + C_{p,o}^2 + C_{p,e}^2$$
$$= 2F_p + \frac{p^r - 1}{2}(C_{p,o} + C_{p,e})$$
$$= \frac{p^r + 3}{2} F_p - \frac{p^r - 1}{2} C_p = (m + 2)F_p - mC_p.$$

It follows that

$$SS^{-1} = \frac{m + 1}{2}(F_p + C_p), mC_q + (m - 2)F_q$$
$$+ \left((m + 2)F_p - mC_p, \frac{m - 1}{2}(F_q - C_q)\right)$$
$$+ (C_p + F_p, F_q - C_q) + (C_p, C_q)$$
$$= \left(\frac{m(m + 1)}{2} + \frac{m(m - 1)}{2}\right)(C_p, C_q)$$
$$+ \left\{\frac{(m + 1)(m - 2)}{2} + \frac{(m + 2)(m - 1)}{2} + 1\right\}(F_p, F_q)$$
$$= m^2(C_p, C_q) + (m^2 - 1)G$$

which again shows that S is a difference set in G with the parameters

$$v = 4m^2 - 1, \quad k = 2m^2 - 1, \quad \lambda = m^2 - 1, \quad n = m^2$$

thereby completing the proof of the theorem.

4. A simpler description of the difference set is possible in the case where $2m+1$ and $2m-1$ are both primes. We have then the following

THEOREM 2. *If two consecutive odd numbers p, q are primes, then the set S consisting of*

(i) *the prime residue classes z (mod pq) such that*

$$\left(\frac{z}{pq}\right) = 1,$$

where

$$\left(\frac{a}{b}\right)$$

is the Jacobi symbol, and

(ii) *the residue classes pz (mod pq), if $p \equiv 1$ (mod 4), or the residue classes qz (mod pq) if $q = 1$ (mod 4), is a difference set in the additive group of residues (mod pq), having the parameters*

$$v = 4m^2 - 1, k = 2m^2 - 1, \lambda = m^2 - 1, n = m^2.$$

PROOF. Any prime residue class z (mod pq) can be written in the form

$$z = px + qy$$

where x and y are prime residue classes (mod q) and (mod p) respectively. Now

$$\left(\frac{z}{pq}\right) = \left(\frac{px + qy}{p}\right)\left(\frac{px + qy}{q}\right)$$
$$= \left(\frac{qy}{p}\right)\left(\frac{px}{q}\right) = \left(\frac{q}{p}\right)\left(\frac{p}{q}\right)\left(\frac{y}{p}\right)\left(\frac{x}{q}\right) = \left(\frac{x}{q}\right)\left(\frac{y}{p}\right),$$

since one of p, q is of the form $4l+1$. Hence

$$\left(\frac{z}{pq}\right) = 1$$

if and only if either both x, y are quadratic residues or both nonresidues mod q, mod p respectively.

It follows that in the decomposition of the additive group of residues z (mod pq) into the direct product of the additive groups of residues (mod q) and (mod p) respectively defined by

$$z \rightarrow (y, x),$$

the set of residues z (mod pq) for which

$$\left(\frac{z}{pq}\right) = 1$$

goes into the union of the sets

$$(C_{p,o}, C_{q,o}), (C_{p,e}, C_{q,e})$$

where $C_{p,e}$, $C_{p,o}$ are the sets of quadratic residues, nonresidues, respectively of p and $C_{q,e}$, $C_{q,o}$ are the sets of quadratic residues, nonresidues respectively of q.

Under the correspondence pz (mod pq) goes into $(0, z)$:

$$pz \rightarrow (0, z)$$

and qz (mod pq) goes into $(z, 0)$:

$$qz \rightarrow (z, 0).$$

It follows that the whole set of residues pz (mod pq) corresponds to the set

$$(C_p, F_q)$$

and the set of residues qz (mod p) corresponds to the set

$$(F_p, C_q)$$

where F_p, F_q are the additive groups of residues mod p, mod q respectively and C_p, C_q are their subsets consisting of their zeros only. Thus the set S in the theorem corresponds to the union of

$$(C_p + C_{p,o}, C_{q,o}), \quad (C_p + C_{p,e}, C_{q,e}), \quad (C_p, C_q)$$

in case $p \equiv 1$ (mod 4), and to the union of

$$(C_{p,o}, C_q + C_{q,o}), \quad (C_{p,e}, C_q + C_{q,e}), \quad (C_p, C_q)$$

in case $q \equiv 1$ (mod 4) which is, in either case, a difference set in the group (F_p, F_q), by Theorem 1. The set S is therefore itself a difference set in the additive group of residues (mod pq).

NEW DELHI, INDIA