Statistica Sinica **27** (2017), 1715-1724
doi:https://doi.org/10.5705/ss.202016.0254

CIRCULANT PARTIAL HADAMARD MATRICES: CONSTRUCTION VIA GENERAL DIFFERENCE SETS AND ITS APPLICATION TO fMRI EXPERIMENTS

Yuan-Lung Lin[1], Frederick Kin Hing Phoa[1] and Ming-Hung Kao[2]

[1]*Academia Sinica and* [2]*Arizona State University*

Abstract: An $m \times n$ matrix $\boldsymbol{A} = (a_{i,j})$ is *circulant* if $a_{i+1,j+1} = a_{i,j}$ where the subscripts are reduced modulo n. A question arising in stream cypher cryptanalysis is reframed as follows: For given n, what is the maximum value of m for which there exists a circulant $m \times n$ (± 1)-matrix $\boldsymbol{A}$ such that $\boldsymbol{A}\boldsymbol{A}^T = n\boldsymbol{I}_m$. In 2013, Craigen et al. called such matrices circulant partial Hadamard matrices (CPHMs). They proved some important bounds and compiled a table of maximum values of m for small n via computer search. The matrices and algorithm are not in the literature. In this paper, we introduce *general difference sets* (GDSs), and derive a result that connects GDSs and CPHMs. We propose an algorithm, the *difference variance algorithm* (DVA), which helps us to search GDSs. In this work, the GDSs with respect to CPHMs listed by Craigen et al. when $r = 0, 2$ are found by DVA, and some new lower bounds are given for the first time.

Key words and phrases: Circulant partial hadamard matrices, functional magnetic resonance imaging (fMRI), general difference sets.

1. Introduction

Difference sets play a crucial role in combinatorial design theory, and provide powerful tools for obtaining experimental designs that possess advantageous statistical properties. A well-known application of difference sets is on the construction of symmetric balanced incomplete block designs (SBIBDs) (Andersen (1990); Bose (1939); Wallis (2007)). Difference sets can also be applied to obtain Hadamard matrices (Hadamard (1893)), which are closely connected to SBIBDs, and are widely considered in design of experiments for rendering useful solutions to some challenging problems (Hedayat et al. (1978)). Recently, Kao (2013, 2014) reported a modern application of difference sets in brain imaging studies. In particular, Paley difference sets are applied to obtain optimal designs for functional magnetic resonance imaging (fMRI) experiments. As a major drawback, this difference method works only for limited situations, and fails to find designs for

other cases that might be encountered in practice. Another useful combinatorial construction in design of experiments is the 'r-row-regular circulant partial Hadamard matrix' (Craigen et al. (2013)). An application of these matrices in constructing good fMRI designs is also discussed in (Kao (2015)). With given integers m, n, and r, an m-by-n, r-row-regular CPHM, abbreviated r-$H(m \times n)$, is a ± 1 circulant matrix $\boldsymbol{H}$ with $\boldsymbol{Hj} = r\boldsymbol{j}$ and $\boldsymbol{HH}^T = n\boldsymbol{I}_m$; here, $\boldsymbol{j}$ is an all-ones vector, $\boldsymbol{I}_m$ is an identity matrix of order m, and $\boldsymbol{H}^T$ is the transpose of $\boldsymbol{H}$. When $m = n$, an r-$H(m \times n)$ is a circulant Hadamard matrix that as conjectured by Ryser (1963), may not exist when $n > 4$. For $m < n$, Low et al. (2005) considered an exhaustive computer search to find some 0-$H(m \times n)$ yielding the maximum m for each $n = 4t \leq 52$. However, such a search for obtaining 0-$H(m \times n)$ with the maximum m can be clumsy when n is large. This also largely hinders the usefulness of CPHMs; e.g., in fMRI studies, n can easily be tens or hundreds. A novel, efficient approach is called for.

We present a general combinatorial construction, *general difference set* (GDS), which is useful because it provides a unified framework for r-$H(m \times n)$ and the difference sets that are widely considered in the literature. As is to be seen, the latter constructs are either special cases of GDS or can be constructed by some GDS. We provide the definition and some useful general properties of the GDS. We then work on the GDSs that render r-$H(m \times n)$, which are useful for fMRI studies and such other applications as stream cipher encryption (Low et al. (2005)). Unfortunately, obtaining such GDSs remains a challenging combinatorial problem. To tackle this, we propose an efficient and effective computational approach through a *difference variance algorithm* (DVA). The DVA allows us to efficiently identify useful r-$H(m \times n)$ without much computational effort. For clarity, we focus only on cases where $r = 0$ and 2, but the DVA can also work for other cases.

In Section 2, we provide the definition and some useful properties of the GDS. The connection between the GDS and r-$H(m \times n)$ is established in Section 3. We then describe our proposed algorithm, DVA, for obtaining some useful GDSs in Section 4. Discussion and conclusion are in Section 5.

2. Preliminaries and Definitions

The difference method is a powerful tool for constructing such high-quality experimental designs as BIBDs. A (v, k, λ) difference set defined in $Z_v = \{1, \ldots, v\}$ is a set $D = \{d_1, \ldots, d_k\}$ that is k-subset of Z_v for which every element in

$Z_v \setminus \{v\}$ can be expressed as $d_i - d_j$ for $i \neq j$ in exactly λ ways. It is worth mentioning that Z_v usually denotes the collection of integers from 0 to $v-1$ in the literature, but here we use Z_v to denote the set of integers $1, \ldots, v$. When $(v, k, \lambda) = (4t-1, 2t-1, t-1)$ and v is a prime power, we have the well-known Paley difference set (Paley (1933)) that consists of all the quadratic residues in $GF(v)$ (The Galois field with v elements). Following (Kao (2015)), the Paley difference sets can also be adopted to obtain some 0-$H(m \times n)$, although this was not pointed out in that paper. While this method gives an infinite number of 0-$H(m \times n)$, the value of m for each n may be relatively small compared to the maximum possible m. For example, the Paley difference set can achieve an 0-$H(5 \times 20)$, but the maximum m for this $n = 20$ is $m = 7$ (Craigen et al. (2013); Low et al. (2005)). Clearly, the existence of r-$H(m \times n)$ implies the existence of r-$H((m-1) \times n)$. For a statistical linear model setting, m also corresponds to the number of factors we can orthogonally estimate. Obtaining r-$H(m \times n)$ with a large m is thus of great interest.

In this study, we present a powerful method to construct r-$H(m \times n)$. The main idea is to make use of general difference sets (GDS).

Definition 1. *A $(v, k; \lambda_1, \ldots, \lambda_{v-1})$ GDS is a set $D = \{d_1, \ldots, d_k\}$ of distinct elements of Z_v such that the difference l appears λ_l times in the multiset $\{d_i - d_j \pmod v \mid d_i, d_j \in D,\ i \neq j\}$ for $l = 1, \ldots, v-1$.*

If $\lambda_1, \ldots, \lambda_{v-1}$ are all λ, then the GDS reduces to an ordinary (v, k, λ) difference set, and thus use (v, k, λ) to denote the parameters of GDS when all the λ_s's are equal.

Definition 2. *Let D be a GDS in Z_v. The incidence matrix of D is an $v \times v$ matrix $\mathbf{A} = (a_{i,j})$ with*

$$a_{i,j} = \begin{cases} -1 & \text{if } j \in D + (i-1), \\ +1 & \text{otherwise,} \end{cases}$$

where $D + (i-1) = \{x + (i-1) \mid x \in D\}$ and all elements are reduced modulo v; $i, j = 1, \ldots, v$.

The first row of $\boldsymbol{A}$ is a binary sequence with $a_{i,j} = -1$ where $j \in D$ and all the others are $+1$. Then the information matrix of $\boldsymbol{A}$ can be directly obtained.

Theorem 1. *Let $\boldsymbol{A}$ be the incidence matrix of a $(v, k; \lambda_1, \ldots, \lambda_{v-1})$ GDS. Then $\boldsymbol{M} = \boldsymbol{A}\boldsymbol{A}^T$ is an $v \times v$ circulant matrix with entries $m_{i,j} = v$ when $i = j$ and $m_{i,j} = v - 4k + 4\lambda_l$ when $i \neq j$, where $l = j - i \pmod v$. Furthermore, $\boldsymbol{M} = \boldsymbol{A}^T\boldsymbol{A}$.*

Proof. Let a_i be the ith row of $\boldsymbol{A}$ and $B_i = D + (i-1)$ for $i = 1, \ldots, v$. It is clear that $m_{i,i} = a_i \cdot a_i = v$ and $m_{i,j} = a_i \cdot a_j = a_j \cdot a_i = m_{j,i}$. By the definition, if $B_j = B_i + (j-i) \pmod v$ as $i \neq j$, then we have $|B_i \cap B_j| = \lambda_l$ where $l = j - i \pmod v$. It is easy to verify that $a_{i,s} \cdot a_{j,s} = -1$ if $s \in (B_i \setminus B_j) \cup (B_j \setminus B_i)$, and $a_{i,s} \cdot a_{j,s} = 1$ otherwise. This implies that $m_{i,j} = (+1)[v - (|B_i| + |B_j| - 2|B_i \cap B_j|)] + (-1)(|B_i| + |B_j| - 2|B_i \cap B_j|)$. Since $|B_i| + |B_j| - 2|B_i \cap B_j| = 2k - 2\lambda_l$, we have $m_{i,j} = v - 4k + 4\lambda_l$. In addition, our claim that $M = \boldsymbol{A}\boldsymbol{A}^T = \boldsymbol{A}^T\boldsymbol{A}$ directly follows from the fact that $\boldsymbol{A}$ is a circulant matrix.

Example 1. Consider a set $D = \{1, 2, 3, 5\}$ in Z_8. Since the differences 3 and 5 appear exactly once and the others twice, D is a $(8, 4; 2, 2, 1, 2, 1, 2, 2)$ GDS. Let $\boldsymbol{A}$ be the incidence matrix of D. With Definition 2 and Theorem 1, we obtain the matrix $\boldsymbol{M} = \mathbf{A}\mathbf{A}^T$ as

$$\boldsymbol{M} = \begin{pmatrix} 8 & 0 & 0 & -4 & 0 & -4 & 0 & 0 \\ 0 & 8 & 0 & 0 & -4 & 0 & -4 & 0 \\ 0 & 0 & 8 & 0 & 0 & -4 & 0 & -4 \\ -4 & 0 & 0 & 8 & 0 & 0 & -4 & 0 \\ 0 & -4 & 0 & 0 & 8 & 0 & 0 & -4 \\ -4 & 0 & -4 & 0 & 0 & 8 & 0 & 0 \\ 0 & -4 & 0 & -4 & 0 & 0 & 8 & 0 \\ 0 & 0 & -4 & 0 & -4 & 0 & 0 & 8 \end{pmatrix}.$$

From $\boldsymbol{M}$, one can easily see that an 0-$H(3 \times 8)$ can be formed by cyclically right-shifting the first row, $(-1, -1, -1, 1, -1, 1, 1, 1)$, of A three times. This is because the upper-left 3-by-3 submatrix of $\boldsymbol{M}$ is $8\boldsymbol{I}_3$. By moving this 3-by-3 'window' along the diagonal of $\boldsymbol{M}$, we again have matrices of $8\boldsymbol{I}_3$. This implies that any three consecutive rows of $\boldsymbol{A}$ form an 0-$H(3 \times 8)$, which also is guaranteed by the fact that a cyclic shift of an 0-$H(3 \times 8)$ remains an 0-$H(3 \times 8)$.

A procedure equivalent to that in (Kao (2015)) can be used to obtain the difference set D by adjusting the Paley difference set. It might be a systematic way to get an $0 - H(m \times n)$, but m is generally very small. The exhaustive computer search (Low et al. (2005)) can be used to identify some 0-$H(m \times n)$ with the maximum m, but is inefficient. In what follows, we provide some results for establishing the connection between the GDS and r-$H(m \times n)$ for a general r. We then propose an efficient algorithm for finding such r-$H(m \times n)$ with a large, if not the maximum, m.

3. Main Results

For convenience, here, $\tilde{\mathbf{A}}_m$ denotes an $m \times n$ matrix consisting of the first m rows of an $n \times n$ matrix $\mathbf{A}$. We also use $I_D(\lambda)$ to denote the index α such that $\lambda_1, \ldots, \lambda_{\alpha-1}$ are all λ, but $\lambda_\alpha \neq \lambda$ where $\alpha > 1$.

Theorem 2. *Let D be a $(n, k; \lambda_1, \ldots, \lambda_{n-1})$ GDS, where $n \equiv 0 \pmod 4$, and let $\boldsymbol{A}$ be its incidence matrix. Then α is the maximum number of rows such that $\tilde{\boldsymbol{A}}_\alpha$ is an r-$H(\alpha \times n)$ if and only if $k = (n - r)/2$ and $I_D((n - 2r)/4) = \alpha$. Furthermore, $\tilde{\boldsymbol{A}}_{\alpha+1}$ is not an r-$H((\alpha + 1) \times n)$.*

Proof. By Theorem 1, if $\tilde{\boldsymbol{A}}_\alpha$ is an r-$H(\alpha \times n)$ with the ith row a_i, then $0 = a_i \cdot a_j = n - 4k + 4\lambda_{j-i}$ for $i \neq j$. Since each row sum of $\boldsymbol{A}$ equals r, we have $k = (n - r)/2$. It follows that $\lambda_{j-i} = (n - 2r)/4$ for $1 \leq i, j \leq \alpha$ and $i \neq j$, so $I_D((n - 2r)/4) = \alpha$.

Conversely, since $I_D((n - 2r)/4) = \alpha$, we have $\lambda_i = (n - 2r)/4$ for all $i = 1, \ldots, \alpha - 1$, but $\lambda_\alpha \neq (n-2r)/4$. In addition, each row of $\boldsymbol{A}$ contains $(n-k)$ $(+1)$'s and k (-1)'s, so that the row sums of $\boldsymbol{A}$ are $(n-k)-k = n-2((n-r)/2) = r$. It is also clear that we have $\tilde{\boldsymbol{A}}_\alpha \boldsymbol{j}_n = r\boldsymbol{j}_\alpha$. Moreover, from Theorem 1, the (i, i)-entry of $\tilde{\boldsymbol{A}}_\alpha \tilde{\boldsymbol{A}}_\alpha^T$ is n, and its (i, j)-entry is $n - 4((n - r)/2) + 4\lambda_{j-i} = n - 2(n - r) + (n - 2r) = 0$ when $i \neq j$. It follows that $\tilde{\boldsymbol{A}}_\alpha$ is an r-$H(\alpha \times n)$. Because $\lambda_\alpha \neq \lambda_{\alpha-1}$, it is clear that $\tilde{\boldsymbol{A}}_{\alpha+1}$ is not an r-$H((\alpha + 1) \times n)$.

For clarity, we focus on the cases $r = 0$ and $r = 2$. Then Theorem 2 has the following corollary.

Corollary 1. *Let D be a $(n, k; \lambda_1, \ldots, \lambda_{n-1})$ GDS, where $n \equiv 0 \pmod 4$, and let $\tilde{\boldsymbol{A}}$ be the incidence matrix of D. Then*

(i) *If $k = n/2$ and $I_D(n/4) = \alpha$, $\tilde{\boldsymbol{A}}_\alpha$ is an 0-$H(\alpha \times n)$.*

(ii) *If $k = (n/2) - 1$ and $I_D((n/4) - 1) = n/2$, $\tilde{\boldsymbol{A}}_{n/2}$ is an 2-$H((n/2) \times n)$.*

Consider the theoretical upper bound of α. From the definition of GDS, it is obvious that $\lambda_l = \lambda_{n-l}$ because the frequencies of $l = i - j$ and $-l = j - i$ are the same. Once $\lambda_1, \ldots, \lambda_{n/2}$ are all λ, all λ_l must equal λ. This implies that an r-$H(\alpha \times n)$ can be extended to be an r-$H(n \times n)$ if $\alpha > n/2$. However, this contradicts Ryser's conjecture. If Ryser's conjecture were true, then $\alpha \leq n/2$. It can be easily proved that the equality holds only if $r = 2$ by counting the allocation of lambdas. Craigen et al. (2013) has proven that $m < n/2$ as $r = 0$ by linear algebra, it can also be proven by a discussion of differences.

There might be many GDSs having the same parameters, resulting in multiple r-$H(m \times n)$. In Table 2, we list the GDS for obtaining r-$H(m \times n)$ when

$8 \leq n \leq 76$ and $r = 0, 2$. In fMRI experiment, the model matrix for estimating HRF can be viewed as the transpose of an r-$H(m \times n)$, so r is relevant to the treatment setting of each effect. We only consider the cases $r = 0, 2$ in order to avoid the bias of the estimation in practice. In fact, we can find more if $r > 2$. These GDSs are obtained by using an efficient computer algorithm introduced in the next section. With our algorithm, practitioners can easily construct CPHMs.

4. Difference Variance Algorithm

We propose an efficient algorithm for searching the GDSs of the required r-$H(m \times n)$. We define a function f that maps a GDS to the frequency of occurrence of each difference. In particular, let $\mathcal{D}$ be a collection of all k-subsets of Z_n. Define $f : \mathcal{D} \to \mathcal{N}^{n-1}$ by $D \mapsto (\lambda_1, \ldots, \lambda_{n-1})$ where $\mathcal{N}$ is the non-negative integers. Define **SP** as a circulant matrix of order n with the first row $(0, 1, \ldots, n-1)$. If all elements in Z_n are considered as the ordered vertices on a ring, then the value of each entry (x, y) in **SP** is the shortest distance between x and y, or $y - x (\mathrm{mod}\ n)$. Let $\mathbf{SP}[D]$ be a matrix constructed by deleting the jth column and row of **SP** for all $j \in Z_n \setminus D$. Each λ_i of $f(D)$ can directly be obtained by counting the frequency the element i in $\mathbf{SP}[D]$. In our algorithm, we use this method to find $f(D)$ for any given $D \in \mathcal{D}$. Here is a criterion to determine whether a GDS is good or not under the condition of Theorem 2. Let D be a $(n, k; \lambda_1, \ldots, \lambda_{n-1})$ GDS with $k = (n - r)/2$, and take

$$d_{var}(D, M) = \sum_{i=1}^{M-1} \frac{(M - i)(\lambda_i - ((n - 2r)/4))^2}{M - 1}, \tag{4.1}$$

where M is a possible maximum value of m such that an r-$H(m \times n)$ exists. Equation (4.1) evaluates the weighted least-square distance from the optimal condition $\lambda_i = (n-2r)/4$. The order of $f(D)$ is significant, because it corresponds to the value of $I_D((n - 2r)/4)$ in Theorem 2. Hence, we set the weight $M - i$ for each term. If $d_{var}(D, M) = 0$, then the corresponding incidence matrix $\tilde{\boldsymbol{A}}_M$ is an r-$H(M \times n)$ and $I_D((n - 2r)/4) = M$. Thus, d_{var}-value is our objective function. For fixed M in general, the smaller the d_{var}-value is, the bigger the m we get.

As a toy example, we evaluate the d_{var}-value of all combinations of 0-$H(m \times n)$ when $n = 28$. There are total $40,116,600$ combinations, but only 784 of them attain the maximum value of $m = 9$. By exchanging the signs and shifting the initial vector, there are only 28 distinct 0-$H(9 \times 28)$. However, some of them might be isomorphic. This suggests the difficulty of searching CPHMs when

Table 1. The difference variance algorithm

```
Randomly generate a subest D of Z_n
Evaluate d_var(D, M)
while GM ≠ 0 do
Obtain a class of sets via EXCHANGE operation
Evaluate the d_var-value of each set to get the LM
if LM < GM then
    update the GM and set D
else
    if LM = GM then
        perform the ADJUST operation
    end if
else go to Step 1
end if
end while
```

n is large. Instead of exhaustive search, we propose an algorithm, *difference variance algorithm* (DVA), to find the required GDSs. DVA is an ordinary hill-climbing search that processes breadth-first search from a random starting point in the search space by a greedy algorithm according to d_{var}-value. The DVA is summarized as Table 1.

4.1. Initialization step

Users input three positive integers n, r, and M, where n is a multiple of 4, r could be 0 or 2, and M is a possible maximum value of m such that an r-$H(m \times n)$ exists. Randomly choose $((n-r)/2)-2$ elements from $\{3, \cdots, n\}$ with the elements 1 and 2 to be a set D. Evaluate the $d_{var}(D, M)$ via $f(D)$ and (4.1). The *global maximum* (GM) is the smallest d_{var}-value of all searched sets. In this step, $GM = d_{var}(D, M)$.

4.2. EXCHANGE operation and ADJUST operation

The EXCHANGE operation generates a class of sets by individually exchanging each element in $D \setminus \{1, 2\}$ and its complement except the elements 1 and 2. Therefore, it produces $[(n-1)^2 - (r+1)^2]/4$ different sets. The *local minimum* (LM) is the smallest d_{var}-value of a set in the class.

The ADJUST operation is the most important procedure in DVA. In our experience, EXCHANGE may result in few sets, say $\mathcal{D}'$, whose d_{var}-value are GM, but they still may be used to get smaller d_{var}-value via the EXCHANGE operation. In this, we obtain LM' for each set $D \in \mathcal{D}'$ via EXCHANGE. If

$LM' < GM$, then update the GM and set D. If $LM' \geq LM = GM$, then go to Step 1. The algorithm may get stuck when we have more than two local minimum points in the search space. This procedure may cause these sets D' to switch to each other via EXCHANGE, so we jump to other points in order to avoid getting stuck.

Repeatedly using the EXCHANGE operation, we could get better GDSs from the previous one. In addition, the ADJUST operation helps us to find some specific GDSs and avoid getting stuck. The program will stop generally when we find the required GDSs, but it is allowed to weaken the condition. For example. the condition in Step 3 could be set as $GM > 0.2$. When n is large, it is hard to find the required GDSs. But we may find a good (if not optimal) GDS if we relax the condition.

5. Discussion and Conclusion

Compared to complete enumeration, the general difference set (GDS) is a powerful and efficient tool for the construction of circulant-type designs. We point out the relationship between combinatorial designs and circulant partial Hadamard matrices. We propose a criterion to quantify a GDS and apply it as DVA to find the GDS of an r-$H(m \times n)$. We depict 0-$H(m \times n)$ and 2-$H(m \times n)$ constructed from specific GDSs, and 0-$H(m \times n)$ is proved as universally optimal for estimating the HRF of a stimulus type and for comparing HRFs of two stimulus types (Cheng and Kao (2015)). We have searched the CPHMs when $n > 52$, see Table 2. Many new lower bounds have been discovered.

The results in this study are useful for fMRI experiments with two stimulus types when the objective is to estimate the contrasts between HRFs. How to extend the current result to designs of fMRI experiments with three or more stimulus types remains an open question. In addition, although the current search of CPHMs is much faster than complete enumeration, it may be possible to further speed up the search via such parallel computing techniques as particle swarm optimization.

Acknowledgment

The authors deeply appreciate the careful corrections and constructive suggestions of an associate editor and two reviewers. This work was supported by Career Development Award of Academia Sinica (Taiwan) grant number 103-CDA-M04, and Ministry of Science and Technology (Taiwan) grant numbers

Table 2. GDS for Constructing r-$H(m \times n)$ for $n \leq 76$.

n	r	max m	General difference set
8	0	3	{1, 2, 3, 5}
8	2	4	{1, 2, 4}
12	0	5	{1, 2, 3, 6, 10, 12}
12	2	6	{1, 2, 3, 5, 10}
16	0	7	{1, 2, 3, 4, 6, 7, 9, 13}
16	2	8	{1, 2, 3, 5, 6, 8, 12}
20	0	7	{1, 6, 7, 10, 12, 14, 15, 16, 17, 18}
20	2	10	{1, 2, 3, 4, 6, 10, 15, 17, 18}
24	0	9	{1, 2, 3, 5, 6, 7, 10, 12, 13, 20, 21, 23}
24	2	12	{1, 2, 3, 4, 6, 8, 11, 12, 19, 21, 22}
28	0	9	{1, 2, 4, 5, 7, 13, 14, 18, 21, 22, 23, 24, 26, 28}
28	2	14	{1, 2, 3, 4, 5, 7, 9, 10, 13, 14, 20, 22, 25}
32	0	12	{1, 2, 3, 7, 13, 14, 16, 19, 21, 23, 24, 25, 26, 27, 30, 31}
32	2	14	{1, 3, 5, 8, 9, 17, 18, 20, 22, 23, 26, 27, 28, 29, 30}
36	0	14	{1, 5, 7, 14, 16, 17, 18, 19, 22, 24, 25, 27, 28, 29, 31, 32, 35, 36}
36	2	18	{1, 2, 3, 4, 5, 8, 9, 11, 13, 14, 16, 17, 18, 24, 28, 30, 33}
40	0	17	{1, 2, 3, 6, 9, 15, 16, 17, 22, 25, 26, 27, 29, 30, 32, 34, 36, 37, 38, 40}
40	2	20	{1, 2, 4, 5, 6, 8, 10, 11, 12, 15, 17, 18, 19, 20, 23, 29, 33, 34, 36}
44	0	16	{1, 2, 3, 4, 5, 6, 10, 11, 13, 14, 15, 17, 18, 20, 21, 23, 29, 31, 35, 36, 40, 42}
44	2	18	{1, 2, 5, 6, 7, 9, 11, 12, 15, 17, 18, 19, 20, 21, 23, 24, 28, 30, 35, 37, 38}
48	0	17	{1, 2, 3, 4, 5, 6, 7, 9, 10, 13, 16, 17, 18, 22, 26, 28, 31, 32, 33, 39, 40, 42, 45, 47}
48	2	24	{1, 3, 5, 6, 7, 8, 10, 11, 14, 16, 17, 18, 19, 22, 23, 24, 26, 33, 36, 37, 39, 44, 45}
52	0	20	{1, 2, 3, 4, 5, 6, 7, 8, 9, 13, 15, 16, 19, 20, 23, 25, 28, 31, 36, 37, 38, 42, 44, 46, 47, 51}
52	2	26	{1, 3, 6, 7, 8, 9, 10, 12, 15, 16, 18, 19, 20, 23, 24, 25, 26, 28, 30, 37, 39, 40, 43, 47, 48}
56	0	23(*)	{1, 3, 5, 6, 9, 10, 11, 12, 13, 14, 18, 20, 21, 22, 23, 25, 26, 27, 28, 32, 38, 39, 43, 46, 47, 49, 52, 55}
56	2	28	{1, 2, 4, 5, 6, 7, 8, 12, 14, 15, 17, 18, 20, 22, 23, 24, 26, 27, 31, 37, 38, 39, 44, 47, 49, 53, 56}
60	0	18(*)	{1, 2, 3, 5, 7, 9, 10, 12, 13, 15, 16, 17, 18, 21, 22, 25, 27, 28, 29, 30, 38, 42, 45, 47, 48, 49, 52, 53, 54, 59}
60	2	30	{1, 2, 3, 4, 5, 6, 8, 10, 12, 13, 15, 16, 19, 22, 23, 24, 27, 28, 29, 37, 39, 41, 44, 47, 48, 50, 55, 56, 60}
64	0	17(*)	{1, 2, 6, 7, 8, 10, 12, 13, 15, 17, 18, 19, 21, 22, 25, 28, 30, 31, 32, 33, 35, 36, 40, 48, 49, 53, 54, 56, 60, 62, 63, 64}
64	2	32	{1, 2, 3, 4, 5, 7, 9, 11, 14, 15, 16, 19, 20, 21, 22, 24, 27, 28, 30, 31, 40, 42, 44, 45, 49, 50, 55, 57, 58, 61, 64}
68	0	17(*)	{1, 2, 3, 4, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 20, 25, 27, 29, 31, 36, 37, 40, 41, 46, 48, 49, 52, 54, 56, 57, 59, 62, 63, 66}
68	2	18(*)	{1, 4, 5, 7, 8, 10, 11, 12, 15, 19, 20, 21, 24, 25, 26, 27, 29, 33, 37, 39, 44, 50, 52, 53, 54, 55, 57, 60, 61, 62, 63, 64, 67}
72	0	17(*)	{1, 2, 3, 5, 6, 7, 9, 11, 12, 13, 14, 15, 18, 19, 22, 23, 28, 29, 31, 37, 39, 40, 43, 45, 50, 52, 55, 56, 57, 59, 60, 62, 63, 64, 70, 72}
72	2	16(*)	{1, 4, 5, 7, 8, 9, 11, 12, 13, 14, 15, 16, 17, 22, 23, 26, 28, 29, 33, 35, 37, 38, 43, 46, 47, 49, 54, 59, 60, 62, 64, 66, 67, 68, 69}
76	0	17(*)	{1, 2, 7, 8, 9, 11, 15, 18, 19, 20, 22, 23, 24, 29, 33, 34, 39, 41, 46, 47, 48, 49, 50, 51, 52, 54, 55, 56, 58, 59, 61, 62, 64, 67, 70, 71, 73, 75}
76	2	38	{1, 2, 4, 5, 6, 7, 9, 11, 12, 17, 21, 23, 24, 30, 32, 33, 34, 38, 41, 46, 48, 51, 52, 53, 54, 56, 57, 58, 60, 63, 64, 65, 66, 67, 69, 73, 74}

104-2118-M-001-016-MY2 and 105-2118-M-001-007-MY2.

References

Andersen, I. (1990). *Combinatorial Designs: Construction Methods*. Ellis Horwood, Chichester and New York.

Bose, R. C. (1939). On the construction of balanced incomplete block designs. *Annals of Eugenics* **9**, 353–399.

Cheng, C.-S. and Kao, M.-H. (2015). Optimal experimental designs for fMRI via circulant biased weighing designs. *The Annals of Statistics* **6**, 1184–1238.

Craigen, R., Faucher, G., Low, R. and Wares, T. (2013). Circulant partial Hadamard matrices. *Linear Algebra and its Applications* **439**, 3307–3317.

Hadamard J. (1893). Resolution d'une question relative aux determinants. *Bull. Des Sciences Math.* **17**, 240–246.

Hedayat, A. and Wallis, W. et al. (1978). Hadamard matrices and their applications. *The Annals of Statistics* **6**, 1184–1238.

Kao, Ming-Hung. (2013). On the optimality of extended maximal length linear feedback shift register sequences. *Statistics & Probability Letters* **83**, 1479–1483.

Kao, Ming-Hung. (2014). A new type of experimental designs for event-related fMRI via Hadamard matrices. *Statistics & Probability Letters* **84**, 108–112.

Kao, Ming-Hung. (2015). Universally optimal fMRI designs for comparing hemodynamic response functions. *Statistica Sinica* **25**, 499–506.

Low, R., Stamp, M., Craigen, R. and Faucher, G. (2005). Unpredictable binary strings. *Congressus Numerantium* **117**, 65.

Paley, R. E. (1933). On orthogonal matrices. *J. Math. Phys.*, 311–320.

Ryser, H. J. (1963). *Combinatorial Mathematics*. New York.

Wallis, W. D. (2007). *Introduction to Combinatorial Designs 2nd ed.* Chapman & Hall/CRC.

Institute of Statistical Science, Academia Sinica, Taipei, Taiwan, R.O.C.

E-mail: gaussla@stat.sinica.edu.tw

Institute of Statistical Science, Academia Sinica, Taipei, Taiwan, R.O.C.

E-mail: fredphoa@stat.sinica.edu.tw

School of Mathematics and Statistical Sciences, Arizona State University, Tempe, Arizona 85287, USA

E-mail: ming-hung.kao@asu.edu

(Received May 2016; accepted August 2016)