On the Non-Existence of Some Generalized Hadamard Matrices

Charlie H. Cooke and Iem Heng

Department of Mathematics and Statistics
Old Dominion University
Norfolk, Virginia 23508, USA

Abstract

A conjecture for generalized Hadamard matrices over group G of order p states that Hadamard matrix $GH(p,h)$ exists only if the matrices I_n and nI_n are Hermitian congruent [1], where $n = ph$ and p is prime. References [4,5] document many parameter values for which non-existence is known to occur. Here, methods for establishing non-existence based upon a fundamental necessary condition of Brock [2] are considered. Several parameter sequences for which non-existence occurs are identified. The methods exploited complement de Launey's [6] approach via number theoretic properties of the Hadamard determinant. Neither investigation is exhaustive of all possibilities.

1 Introduction

Let C_s be the multiplicative group of all complex s^{th} roots of unity. The square matrix $H = [h_{ij}]$ of order r over C_s is said to be a "*Butson Hadamard matrix*", briefly a $BH(s,r)$ matrix, if and only if $HH^* = rI_r$. Here, H^* is the conjugate transpose of H.

$BH(2,r)$ matrices are referred to simply as Hadamard matrices (or ± 1 matrices). Such matrices exist only if $r = 1, 2$ or else $r = 4k$, where k is a positive integer. Existence has been verified for at least each and every $k \leq 106$, and the classical Hadamard conjecture states that existence occurs for each integer $k > 0$.

For primes $p > 2$, the situation is quite different. A necessary condition for the existence of $BH(p > 2, r)$ is that $r = pt$, where t is a positive integer. This condition is also sufficient, for the case of $BH(p > 2, 2^m p^k)$, provided $0 \leq m \leq k$, where k is an integer [3].

It has been conjectured [1] that $BH(p, pt)$ exists, for primes $p > 2$ and all positive integers t. However, instances have been discovered where this conjecture fails [4].

The most recent generalized Hadamard conjecture[6] is that $H(p,n)$ exists only if I_n is Hermitian congruent to nI_n, where $n = pt$.

In this paper techniques are explored for proving non-existence of infinite sequences of potential $BH(s, r_k)$, $k \in K$, where K is a countably infinite set of positive integers. Sets K are identified for which $\{BH(s, r_k) : k \in K\} = \phi$. These techniques consist chiefly of methods for proving non-existence of non-trivial solutions to homogeneous Diophantine equations

$$ax^2 + by^2 + cy^2 = 0.$$

2 Hadamard Matrices Over Groups

Definition 1: Let $(G, \odot)$ be a group of order g. A $(g, k; \lambda)$-difference matrix is a $k \times g\lambda$ matrix $D = (d_{ij})$ with entries from G, such that for each $1 \leq i < j \leq k$, the multiset

$$\{d_{il} \odot d_{jl}^{-1} : 1 \leq l \leq g\lambda\}$$

contains every element of G λ times. When G is Abelian, typically, additive notation is used, so that differences $d_{il} - d_{jl}$ are employed.

Consider the additive group $G = \{0, 1, 2\}$ with modulo three arithmetic. Two inequivalent $(3, 6; 2)$-difference matrices over G are

$$A = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 2 & 2 \\ 0 & 1 & 0 & 2 & 2 & 1 \\ 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 2 & 2 & 1 & 0 & 1 \\ 0 & 2 & 1 & 2 & 1 & 0 \end{bmatrix}$$

and

$$B = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 2 & 0 & 1 \\ 1 & 0 & 2 & 2 & 1 & 0 \\ 0 & 2 & 2 & 0 & 1 & 1 \\ 2 & 2 & 0 & 1 & 1 & 0 \\ 2 & 0 & 2 & 1 & 0 & 1 \end{bmatrix}.$$

Definition 2: A generalized Hadamard matrix $GH(g, \lambda)$ over group G is a $(g, g\lambda; \lambda)$-difference matrix [4].

A number of authors have studied these matrices [7], [8], [11], [12], [13], and [14]. For a summary of the known matrices, see Theorem A of Street [14].

Clearly, both difference matrices A and B are generalized Hadamard matrices $GH(3,2)$, each having an associated Butson Hadamard matrix $BH(3,6)$. This association will now be clarified.

Theorem 1 *For primes $p > 2$, there exists a generalized Hadamard matrix $BH(p, p\lambda)$ over the cyclic group C_p if and only if there exists a generalized Hadamard matrix $GH(p,\lambda)$ over the additive group $Z_p = \{0, 1, 2, ..., p-1\}$, (+).*

A generalization of this result is stated by Drake [7], whose proof follows from results of Butson [3]. This association will be illustrated by example.

Let $C_3 = \{1, x, x^2\}$, where $x = e^{2\pi i/3}$ is a primitive cube root of unity. Consider the BH-matrices

$$H = BH(3,6) = x^E$$

where E is one of the difference matrices A, B above. The notation means that matrix elements obey $h_{ij} = x^{e_{ij}}$.

By calculation, $HH^* = 6I$; therefore, H is a generalized Hadamard matrix in the classical sense. Also, by calculation H is a $GH(3,2)$ matrix with respect to $C_3, \odot$. The Hadamard exponent forms (matrices A, B above) have already been cited as $GH(3,2)$ with respect to the group $Z_3, \oplus$.

The next theorem provides a necessary condition for the existence of $GH(g,\lambda)$ over group G, $|G| = g$:

Theorem 2 *A $GH(g,\lambda)$ with $n = g\lambda$ odd exists over Abelian group G of order $|G| = g$ only if a nontrivial solution in integers x,y,z exists to the quadratic Diophantine equation*

$$z^2 = nx^2 + (-1)^{(t-1)/2}ty^2,$$

for every order, t, of a homomorphic image of G.

The proof of this theorem can be found in Brock [2], and it is discussed in Colbourn and Dinitz [4].

Corollary 1 *For primes $p > 2$, and $\lambda > 0$ an odd integer, $BH(p, p\lambda)$ exists only if there are nontrivial solutions in integers to both equations*

$$z^2 = p\lambda x^2 + (-1)^{(p-1)/2}py^2$$

and

$$z^2 = p\lambda x^2 + y^2.$$

Proof. If G is an Abelian group of order $p > 2$, where p is prime, there exist homomorphic images of G of orders $t = 1, p$. □

3 The Imbedding Problem

Definition 3: Let G be an Abelian group of order g, with $n = g\lambda$, where λ is a positive integer. For $0 < k < n$, a $k \times n$ difference matrix D over the group G is "completable" if and only if there exists a $GH(g, \lambda)$ matrix having D as its first k rows.

The Hadamard imbedding problem concerns the question of whether the matrix D can be extended by the process of row addition so as to be completable. This problem has been studied variously by Beder [1], Brock [2], Drake [7] and others.

Definition 4: Difference matrix D of dimension $k \times n$ is "locally maximal" (in dimension) if there is no $(k+1) \times n$ difference matrix which reduces to D by deletion of a single row. If D is a $GH(g, \lambda)$, then it is globally maximal [4].

It is interesting to note that there may exist locally maximal $(g, k; \lambda)$-difference matrices for which $k < g\lambda$, even in cases where a $(g, g\lambda; \lambda)$-difference matrix exists. For $g = 2$ and $\lambda = 10$, Beder [1] constructs such (± 1) matrices, characterized by $k = 8, 12, 16$.

With respect to the group $G = \{0, 1, 2\}$, $(+)$, the present authors have discovered locally maximal difference matrices $D_{k \times 15}$ with $k = 7, 8$ (see Tables I and II). The observation that $gcd(7, 15) = gcd(8, 15) = 1$ appears a stark contrast to what may be observed in Beder's (± 1) difference matrices; namely, in cases where locally maximal difference matrices of dimension $D_{k \times n}$ and $D_{n \times n}$ simultaneously exist, $gcd(k, n) \neq 1$ (for $n = 20$; $k = 8, 12, 16$).

This contrasting behaviour leads to the likely conjecture that $GH(3, 15)$ does not exist. Actually, this has been known for several years. However, following up this conjecture in absence of this knowledge motivated the present research on non-existence of certain $GH(g, \lambda)$.

Tables I and II show the previously referred to locally maximal difference matrices with respect to group $G = \{0, 1, 2\}$, $(+)$:

$$\begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 2 \\
0 & 0 & 1 & 1 & 1 & 2 & 2 & 0 & 0 & 0 & 1 & 1 & 2 & 2 & 2 \\
0 & 0 & 1 & 1 & 2 & 1 & 0 & 2 & 2 & 0 & 2 & 2 & 1 & 1 & 0 \\
0 & 0 & 1 & 2 & 2 & 0 & 1 & 1 & 2 & 2 & 1 & 0 & 2 & 0 & 1 \\
0 & 1 & 2 & 0 & 2 & 1 & 2 & 0 & 1 & 2 & 1 & 0 & 1 & 2 & 0 \\
0 & 1 & 0 & 2 & 2 & 2 & 1 & 2 & 1 & 0 & 0 & 1 & 1 & 0 & 2
\end{bmatrix}$$

Table I
A (3,7,15)-difference matrix

$$\begin{bmatrix} 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&1&2&1&2&1&2&1&2&1&2&0&0&0&0\\ 0&2&1&1&1&1&1&2&0&2&0&2&2&0&0\\ 0&1&2&2&2&0&1&2&1&0&0&1&1&2&0\\ 0&2&1&1&0&2&1&0&2&0&2&1&0&2&1\\ 0&1&2&0&1&2&0&2&0&1&1&2&0&2&1\\ 0&2&0&0&1&2&2&1&1&0&2&2&1&1&0\\ 0&1&0&2&1&2&1&0&2&1&0&0&2&1&2 \end{bmatrix}$$

Table II
A (3,8,15)-difference matrix

4 Quadratic Diophantine Equations

We now consider methods for establishing non-existence of nontrivial integer solutions to the homogeneous Diophantine equation

$$ax^2 + by^2 + cz^2 = 0. \tag{1}$$

Lemma 1 *If a and b are integers, then the equation*

$$z^2 = abx^2 \pm ay^2$$

has nontrivial integer solutions only if the reduced equation

$$a\ell^2 = bx^2 \pm y^2$$

has nontrivial integer solutions.

Proof. The result is obvious. If (x, y, z) is a solution, of necessity $a|z$. Therefore, let $z = a\ell$, where ℓ is an integer if z is. □

Method I:

Legendre's Theorem: [10]

Let a, b, c be pairwise relatively prime integers which are squarefree and not all of the same algebraic sign. Then equation (1) has a nontrivial solution in the integers if and only if $-bc$, $-ac$, $-ab$ are quadratic residues of a, b, c, respectively.

Warwick de Launey [6] has approached the non-existence question for generalized Hadamard matrices by means of number theoretic properties of the Hadamard determinant. Basically, he proves the non-existence of many generalized Hadamard matrices for groups whose orders are divisible by 3,5 or 7; for example, $GH(15, C_{15})$, $GH(15, C_3)$, and $GH(15, C_5)$.

That his work is non-exhaustive is evidenced by the following result:

Theorem 3 *For Abelian groups of order p, and for odd primes $p \equiv \pm 3 (mod\ 5)$, $GH(p, 5)$ does not exist.*

Proof. Consider the problem of finding integer solutions to the equation

$$z^2 = 5px^2 \pm py^2, \tag{2}$$

where $p \equiv \pm 3(mod\ 5)$. This can be done only if one can find integer solutions of

$$pq^2 = 5x^2 \pm y^2 \tag{3}$$

As $x^2 \equiv \pm 3(mod\ 5)$ has no solutions, by Legendre's theorem neither does (2) or (3) have nontrivial integer solutions. □

Note. Clearly, theorem 3 generalizes some of de Launey's results.

5 Reciprocity

Definition 5: For groups G, H with $|G| = g$ and $|H| = \lambda$, potential generalized Hadamard matrices $GH(g, \lambda)$ and $GH(\lambda, g)$ satisfy a reciprocity relation provided both exist or both do not exist.
Example. $GH(3, 5)$ and $GH(5, 3)$ are reciprocally non-existent, as in each case the pertinent reduced equation is of the form

$$5a^2 = 3b^2 + c^2.$$

By Legendre's theorem, this equation has no nontrivial integer solutions (a, b, c), since ± 3 is a quadratic non-residue of 5.
By the same approach, the following result can be established:

Theorem 4 *Let λ be a prime number. If $(-1)^{\frac{5+1}{2}}\lambda$ and $(-1)^{\frac{\lambda-1}{2}}\lambda$ are both quadratic non-residues of 5, or if $(-1)^{\frac{5+1}{2}}5$ and $(-1)^{\frac{\lambda-1}{2}}5$ are both quadratic non-residues of λ, then $GH(5, \lambda)$ and $GH(\lambda, 5)$ constitute a reciprocally non-existent pair.*

Corollary 2 *If $7 + 5k$ is a prime number, then $GH(5, 7 + 5k)$ and $GH(7 + 5k, 5)$ constitute a reciprocally non-existent sequence of potential generalized Hadamard matrices.*

Theorem 5 *Let $p = 4k + 3$ and $q = 4k + 5$ be prime numbers, where 2 is a quadratic non-residue of p. Then (p, q) is a reciprocal pair.*

Proof. Since p, q are squarefree and relatively prime, Legendre's theorem applies to determine integer solutions of the equations

$$z^2 = pqx^2 - py^2$$

and

$$z^2 = pqx^2 + qy^2.$$

Existence of a nontrivial integer solution of either equation can happen only if there exists a nontrivial integer solution (ℓ, m, n) for equations of the following type

$$p\ell^2 = qm^2 - n^2.$$

No solution for this equation exists, as

$$x^2 \equiv 2(mod\ p)$$

has no solution. □

A more general method for finding reciprocal pairs employs a result of Euler:

Euler's Theorem: [15]
If p is an odd prime which does not divide a, then $x^2 \equiv a(mod\ p)$ has a solution or no solution according as

$$a^{(p-1)/2} \equiv 1(mod\ p)$$

or

$$a^{(p-1)/2} \equiv -1(mod\ p).$$

Reciprocity Theorem: *Let $p = 4k + 3$ and $a = 4l + 5$ be odd primes which satisfy Euler's condition*

$$a^{(p-1)/2} \equiv -1(mod\ p).$$

Then $GH(a, p)$ and $GH(p, a)$ constitute a reciprocal non-existent pair of generalized Hadamard matrices over groups G, H of order p, a.

Proof. Under the hypotheses of the theorem, Euler's condition guarantees the non-existence of non-trivial integer solutions (x, y, z) to both equations

$$z^2 = apx^2 - py^2$$

and

$$z^2 = apx^2 + ay^2,$$

whose reduced equation is of the form

$$p\ell^2 = ax^2 - y^2.$$

□

Several reciprocal pairs are given by Table III:

$$\begin{bmatrix} 3 & 5 \\ 3 & 17 \\ 3 & 29 \\ 11 & 13 \\ 11 & 17 \\ 11 & 29 \\ 19 & 29 \\ 19 & 59 \\ 19 & 79 \\ 59 & 61 \\ 111 & 113 \end{bmatrix}$$

Table III

Method II:

When the hypotheses of Legendre's theorem fail, an analysis of last digit [9] of separate members of equation (1) is sometimes fruitful. Here, if x is a nonzero integer, the last digit of x is denoted by $[x]$. For instance, the last digit of x^2 is in the set

$[x^2] = \{0, 1, 4, 5, 6, 9\}$, and

$[3x^2] = \{0, 2, 3, 5, 7, 8\} = [7x^2]$,

$[(10k + 1)x^2] = [x^2]$, $k \geq 0$ an integer

$[5x^2] = \{0, 5\}$,

$[9x^2] = \{0, 1, 4, 5, 6, 9\}$.

These facts are useful in proving some non-existence theorems below.

Lemma 2 *The equation*

$$z^2 = 3 \cdot 5 \cdot (2k + 1)x^2 - 3y^2 \tag{4}$$

where k is a non-negative integer satisfying $(2k + 1) \not\equiv 0(mod\ 5)$, does not possess a nontrivial solution in integers.

Proof. By the method of contradiction, assume a nontrivial solution (x, y, z) exists, where (x, y, z) are non-negative integers. As the equation is homogeneous of degree two, (x, y, z) is a solution if and only if (tx, ty, tz) is a solution, where t is an integer. Therefore, it can be assumed that $gcd(x, y, z) = 1$.

Clearly, z is divisible by 3. If $z = 3\ell$, where ℓ is an integer, then equation (4) reduces to

$$y^2 = 5(2k+1)x^2 - 3\ell^2. \tag{5}$$

As the last digit of each integer (x^2, y^2, k^2) belongs to the set $L = \{0, 1, 4, 5, 6, 9\}$, the last digits of $5(2k+1)x^2$ and $3\ell^2$ are members of $\{0, 5\}$ and $\{0, 2, 3, 5, 7, 8\}$, respectively. For compatibility with (5), the last digit of y^2 can only be zero or five; therefore, $y = 5m$, where m is an integer.

Now equation (5) becomes

$$3\ell^2 = 5(2k+1)x^2 - 25m^2. \tag{6}$$

Therefore, $\ell = 5p$, where p is an integer. Equation (6) becomes

$$(2k+1)x^2 = 15p^2 + 5m^2.$$

Since five does not divide $2k+1$, it is necessary that $x = 5q$, where q is an integer. The conclusions $5|y$ and $5|x$ imply that $5|z$. As this contradicts $gcd(x, y, z) = 1$, the assumption that (4) has a nontrivial solution in the integers must be false. □

Lemma 3 *The equation*

$$z^2 = 5 \cdot n \cdot (10k+1)x^2 + 5y^2 \tag{7}$$

has no nontrivial solution for integers $k \geq 0$ and $n = 1, 3, 7$.

Proof. By the method of contradiction, assume a nontrivial solution (x, y, z) exists, where (x, y, z) are positive integers. As the equation is homogeneous of degree two, (x, y, z) is a solution if and only if (tx, ty, tz) is a solution, where t is an integer. Therefore, it can be assumed that $gcd(x, y, z) = 1$.

Clearly, z is divisible by 5 in equation (7).

<u>Case 1:</u> $n = 1$

If $z = 5\ell$, where ℓ is an integer, then equation (7) reduces to

$$y^2 = 5\ell^2 - (10k+1)x^2. \tag{8}$$

As the last digit of each integer (x^2, y^2, ℓ^2) belongs to the set $L = \{0,1,4,5,6,9\}$, the last digits of $5\ell^2$ and $(10k+1)x^2$ are members of $\{0,5\}$ and $\{0,1,4,5,6,9\}$, respectively. For compatibility with (8), the last digit of x^2 and y^2 can only be zero or five; therefore, $x = 5m$ and $y = 5p$, where m,p are integers.

The conclusions $5|y$ and $5|x$ imply that $5|z$. As this contradicts $gcd(x,y,z) = 1$, the assumption that (7) has a nontrivial solution in the integers must be false.

Case 2: $n = 3$

If $z = 5\ell$, where ℓ is an integer, then equation (7) reduces to

$$y^2 = 5\ell^2 - 3(10k+1)x^2. \tag{9}$$

As the last digit of each integer (x^2, y^2, ℓ^2) belongs to the set $L = \{0,1,4,5,6,9\}$, the last digits of $5\ell^2$ and $3(10k+1)x^2$ are members of $\{0,5\}$ and $\{0,2,3,5,7,8\}$, respectively. For compatibility with (9), the last digit of y^2 can only be zero or five; therefore, $y = 5m$, where m is an integer.

Now equation (9) becomes

$$3(10k+1)x^2 = 5\ell^2 - 25m^2.$$

Since five does not divide $3(10k+1)$, it is necessary that $x = 5p$, where p is an integer. The conclusions $5|y$ and $5|x$ imply that $5|z$. As this contradicts $gcd(x,y,z) = 1$, the assumption that (7) has a nontrivial solution in the integers must be false.

Case 3: $n = 7$

If $z = 5\ell$, where ℓ is an integer, then equation (7) reduces to

$$y^2 = 5\ell^2 - 7(10k+1)x^2. \tag{10}$$

As the last digit of each integer (x^2, y^2, ℓ^2) belongs to the set $L = \{0,1,4,5,6,9\}$, the last digits of $5\ell^2$ and $7(10k+1)x^2$ are members of $\{0,5\}$ and $\{0,2,3,5,7,8\}$, respectively. For compatibility with (10), the last digit of y^2 can only be zero or five; therefore, $y = 5m$, where m is an integer.

Now equation (10) becomes

$$7(10k+1)x^2 = 5\ell^2 - 25m^2.$$

Since five does not divide $7(10k+1)$, it is necessary that $x = 5p$, where p is an integer. The conclusions $5|y$ and $5|x$ imply that $5|z$. As this contradicts $gcd(x,y,z) = 1$, the assumption that (7) has a nontrivial solution in the integers must be false. □

6 Summary

Theorem 6 *Several sequences of potential Hadamard matrices over Abelian group G of order g which do not exist are:*

1. $GH(3, 5(2k+1))$, $(2k+1) \not\equiv 0 (mod\ 5)$, *with k a non-negative integer,*

2. $GH(5, n(10k+1))$, *for $n = 1, 3, 7$, k non-negative,*

3. $GH(5, p)$, *where $p \equiv \pm 3 (mod\ 5)$ is an odd prime,*

4. *Reciprocal pairs $GH(5, 7+5k)$ and $GH(7+5k, 5)$, where $7+5k$ is an odd prime.*

Corollary 3 *For k a non-negative integer, the following classes of BH matrices do not exist:*

1. $BH(3, 15(2k+1))$, $(2k+1) \not\equiv 0 (mod\ 5)$,

2. $BH(5, 5n(10k+1))$, *for $n = 1, 3, 7$,*

3. $BH(5, 5p)$, $p \equiv \pm 3 (mod\ 5)$, *an odd prime,*

4. *Reciprocal pairs $BH(5, 35+25k)$ and $BH(7+5k, 35+25k)$, where $7+5k$ is an odd prime.*

The following conjecture, which motivated this research, appears to gain some support from Corollary 3 and Tables I and II:

Conjecture 1 *If for $0 < k < g\lambda$ a locally maximal (g, k, λ)-difference matrix with respect to Abelian group G of order g exists for which $gcd(k, g\lambda) = 1$, then $GH(g, \lambda)$ does not exist.*

7 Conclusions

Although the approaches of de Launey and the present author provide many instances of non-existent $GH(p, q)$, these results are by no means exhaustive of all possibilities. The methods usefully complement each other, and together show the number theoretic complexity of this non-existence problem.

Acknowledgment

The authors would like to thank Professor Jennifer Seberry for constructive comments and suggestions.

References

[1] Beder, J.H. (1995). Conjectures about Hadamard matrices, *R.C. Bose Memorial Conference On Statistical Design and Related Combinatorics*, Colorado State University, June 7-11, 1995.

[2] Brock, B.W. (1988). Hermitian congruence and the existence and completion of generalized Hadamard matrices, *J. of Combinatorial Theory (Series A)*, Vol. 49, 233-261.

[3] Butson, J.A. (1963). Relations among generalized Hadamard matrices, *Can. J. Math.*, Vol. 15, 42-48.

[4] Colbourn, C.J. and Dinitz, J.H. (1996). "*The CRC Handbook of Combinatorial Designs*", CRC Press, New York.

[5] Dawson, J. (1985). A construction for generalized Hadamard matrices GH(4q, EA(4q)), *J. Stat. Plann. and Inference*, Vol. 11, 103-110.

[6] de Launey, W. (1984). On the non-existence of generalized Hadamard matrices, *J. Stat. Plann. and Inference*, Vol. 10, 385-396.

[7] Drake, D.A. (1979). Partial λ-geometries and generalized Hadamard matrices over groups, *Can. J. Math.*, Vol. 31, 617-627.

[8] Jungnickel, D. (1979). On difference matrices, resolvable transversal designs and generalized Hadamard matrices, *Math. Z.*, Vol. 167, 49-60.

[9] Private communication, Mark Dorrepaal, Department of Mathematics, Old Dominion University, Norfolk, Virginia.

[10] Ryser, H.J. (1963). "*Combinatorial Mathematics*", Carus Math. Monograph Vol 14. Wiley, New York.

[11] Seberry, J. (1980). A construction for generalized Hadamard matrices, *J. Stat. Plann. and Inference*, Vol. 4, 365-368.

[12] Seberry, J. (1979). Some remarks on generalized Hadamard matrices and theorems of Rajkundlia on SBIBDs, *Combinatorial Mathematics VI*, Lecture Notes In Mathematics Vol. 748. Springer-Verlag, New York.

[13] Shrikhande, S.S. (1964). Generalized Hadamard matrices and orthogonal arrays of strength 2, *Can. J. Math.*, Vol. 16, 736-740.

[14] Street, D. (1979). Generalized Hadamard matrices, orthogonal arrays and F-squares, *Ars Combinatoria*, Vol. 8, 131-141.

[15] Underwood, D. (1969). "*Elementary Number Theory*", W.H. Freeman Company, San Francisco.

(Received 19/3/98)