Application of the discrete Fourier transform to the search for generalised Legendre pairs and Hadamard matrices

Roderick J. Fletcher

8460 Greystone Ln. Apt. 2F
Columbia, Maryland 21045, USA

Marc Gysin

Bullant Technology,
181 Miller Street,
North Sydney, NSW 2060, Australia.

Jennifer Seberry*

Centre for Computer Security Research
School of Information Technology and Computer Science
The University of Wollongong, Wollongong NSW 2522, Australia

Abstract

We introduce Legendre sequences and generalised Legendre pairs (GL–pairs). We show how to construct an Hadamard matrix of order $2\ell + 2$ from a GL–pair of length ℓ. We review the known constructions for GL–pairs and use the discrete Fourier transform (DFT) and power spectral density (PSD) to enable an exhaustive search for GL–pairs for lengths $\ell \leq 47$ and partial searches for other ℓ.

1 Definitions and Notation

Let U be a sequence of ℓ real numbers $u_0, u_1, ..., u_{\ell-1}$. The *periodic autocorrelation function* $P_U(j)$ of such a sequence is defined by:

$$P_U(j) = \sum_{i=0}^{\ell-1} u_i u_{i+j \bmod \ell}, \quad j = 0, 1, ..., \ell - 1.$$

*Research supported by ARC Large Grants A9803826 and A49703117.

Two sequences U and V of identical length ℓ are said to be *compatible* if the sum of their periodic autocorrelations is a constant, say a, except for the 0-th term. That is,

$$P_U(j) + P_V(j) = a, \quad j \neq 0. \tag{1}$$

(Such pairs are said to have *constant periodic autocorrelation* even though it is the sum of the autocorrelations that is a constant.) If U and V are both ± 1 sequences, compatible and $a = -2$, then they are called *a generalised Legendre pair (or GL–pair) of length* ℓ. We will denote a GL–pair of length ℓ by $GL(\ell)$. In Sections 3–5, we restrict our attention to GL–pairs.

An *Hadamard matrix of order* n is an $n \times n$ matrix H which has ± 1–entries and all its rows and columns are orthogonal. In other words

$$HH^T = nI_n$$

where I_n is the identity matrix of order n.

For the definition of *supplementary difference sets* the reader is referred to [WSW72].

We note that two compatible sequences may contain elements from any alphabet. If the elements of two compatible sequences are $0, 1$ then they are described as $2 - \{\ell; k_1, k_2; \lambda\}$ supplementary difference sets (SDS). In this paper we are interested in the particular case of $2 - \{\ell; \frac{\ell+1}{2}, \frac{\ell+1}{2}; \frac{\ell+1}{2}\}$ SDS since these give, when the zeros are replaced by -1, compatible ± 1 sequences which are a $GL(\ell)$–pair, and may be used as below to construct Hadamard matrices of order $2\ell + 2$. The Legendre or Jacobi symbol is written $(a|n)$ if n is prime or composite, respectively. When referring to the elements of a $-1, 0, 1$ sequence we often write '$-$' instead of -1 and '$+$' instead of 1.

The *discrete Fourier transform (DFT)* of a sequence U is given by

$$DFT_U(k) = \mu_k = \sum_{i=0}^{\ell-1} u_i \omega^{ik}, \quad k = 0, 1, ..., \ell - 1$$

where ω is the primitive ℓ-th root of unity $e^{\frac{2\pi i}{\ell}}$. If we take the squared magnitude of each term in the DFT of U, the resulting sequence is called the *power spectral density (PSD)* of U. The k-th terms in the PSDs of U and V are denoted by $|\mu_k|^2$ and $|\nu_k|^2$.

Example 1 The PSD of the sequence 1 2 2 -2 0 0 0 is

$$9.000\ 19.988\ 13.220\ \ 7.792\ \ 7.792\ 13.220\ 19.988\,.$$

If a sequence U is transformed by the operation of cyclically taking every d-th element, where $\gcd(d, \ell) = 1$, the sequence U is said to be *decimated* by d. That is, if $V = U$ decimated by d, then $v_i = u_{di \bmod \ell}$.

Example 2

$$1111000 \text{ decimated by } 2 = 1100110$$
$$1111000 \text{ decimated by } 3 = 1101010.$$

The set of all possible decimations of a sequence is called a *decimation class.* Since d is required to be relatively prime to ℓ, a sequence of length ℓ has $\phi(\ell)$ decimations, where ϕ is the Euler totient function, though sometimes these are not all distinct. We note that decimation by -1 is the same as reversing a sequence. Hence, by assuming that each sequence also represents its reverse, the maximum size of any decimation class is $\phi(\ell)/2$. Finally, we define compatibility between decimation classes. Two decimation classes are said to be compatible if and only if some sequence belonging to one class is compatible with some sequence in the other class.

2 Some Preliminary Results

We make use of the following well-known theorem [PFTV89, Chapter 12], [Tretter76, Chapter 10].

Theorem 1 Wiener–Khinchin Theorem *The PSD of a sequence is equal to the DFT of its periodic autocorrelation function*

$$|\mu_k|^2 = \sum_{j=0}^{\ell-1} P_U(j)\omega^{jk}. \tag{2}$$

The periodic autocorrelation function is equal to the inverse DFT of the sequence's PSD

$$P_U(j) = \frac{1}{\ell}\sum_{k=0}^{\ell-1} |\mu_k|^2\omega^{-jk}. \tag{3}$$

We note that

Theorem 2 *Two sequences are compatible if and only if their PSDs sum to a constant.*

Proof. By straightforward application of (1), (2) and (3), we have

$$\begin{aligned} |\mu_k|^2 + |\nu_k|^2 &= \sum_{j=0}^{\ell-1}(P_U(j) + P_V(j))\omega^{jk} \\ &= (P_U(0) + P_V(0) - a)\omega^0 + \sum_{j=0}^{\ell-1} a\omega^{jk} \\ &= c \quad (k \neq 0) \end{aligned}$$

$$P_U(j) + P_V(j) = \frac{1}{\ell}\sum_{k=0}^{\ell-1}(|\mu_k|^2 + |\nu_k|^2)\omega^{-jk}$$
$$= \frac{1}{\ell}(|\mu_0|^2 + |\nu_0|^2 - c)\omega^0 + \frac{1}{\ell}\sum_{k=0}^{\ell-1} c\omega^{-jk}$$
$$= a \quad (j \neq 0).$$

The inequalities $k \neq 0$ and $j \neq 0$ are required only in the final steps of the above equations in order to force the rightmost sums to vanish.

Example 3 Two compatible sequences and their PSDs are shown below.

Sequences	PSD (terms 1 to 3)			
1 2 2 -2 0 0 0	19.988	13.220	7.792	
2 1 -1 2 -1 0 0	5.012	11.780	17.208	
	25.000	25.000	25.000	(hence c = 25)

In fact, the constant c depends only on the set of numbers comprising the sequences U and V. It is easily shown that

$$c = \frac{\ell\sum_{i=0}^{\ell-1} u_i^2 - (\sum_{i=0}^{\ell-1} u_i)^2}{\ell - 1} + \frac{\ell\sum_{i=0}^{\ell-1} v_i^2 - (\sum_{i=0}^{\ell-1} v_i)^2}{\ell - 1}. \tag{4}$$

Hence, all permutations of the sequences yield the same constant. Theorem 2 is a generalisation of results that have appeared in the literature in other forms.

The following useful relationships are easily proved by direct application of the definitions of decimation, autocorrelation and DFT.

- If a sequence is decimated by d, then its autocorrelation is likewise decimated by d, and its DFT and PSD are decimated by $d^{-1} \bmod \ell$.
- It follows immediately that compatible sequences remain compatible if they are decimated by the same amount.

Remark: If U, V are $(\pm 1, 0)$–sequences then the above constant c is $c = w - a$, where w is the total number of non–zero entries and a is the constant from the periodic autocorrelation function of U and V.

3 Legendre Sequences and Modified Legendre Sequences

For the remainder of this paper we consider only GL–pairs. The following is well known (see for example [WSW72]) and is included for completeness only. Let p be

an odd prime. The $-1, 0, 1$ sequence U of length p is called a *Legendre sequence* L if its elements $u_i = l_i$ satisfy

$$l_i = (i|p).$$

In other words, $l_0 = 0$ and for $i \neq 0$, $l_i = 1$ if i is a square modulo p and $l_i = -1$, otherwise. We call $(-1, L)$, $(0, L)$, or $(1, L)$ a *modified Legendre sequence.* The values of the modified Legendre sequence are exactly the same as those of the unmodified one except for l_0 which is set to -1, 0, or $+1$, respectively. ($(0, L)$ is of course the original Legendre sequence but sometimes it is convenient to refer to it as a modified Legendre sequence.) Two sequences (e_1, L), (e_2, L) with $e_1, e_2 \in \{-1, 0, 1\}$ are called *modified Legendre sequences* and they are defined in the obvious manner.

Example 4 Let $p = 7$. The modified Legendre sequences $(0, L)$ and $(1, L)$ are given by

$$(0, L) = 0 + + - + - -$$
$$(1, L) = + + + - + - - .$$

Lemma 1 *Let p be an odd prime, then $(1, -L)$, $(1, L)$ is a $GL(p)$-pair.*

This lemma shows the existence of a $GL(p)$–pair for every odd prime p. We also note that

Lemma 2 *Let $p = 2\ell + 1$ be a prime power, then there is a $GL(\ell)$-pair.*

Proof. We use the Szekeres difference sets [GerSeb79] A and B with parameters $2 - \{\ell; \frac{\ell+1}{2}, \frac{\ell+1}{2}; \frac{\ell+1}{2}\}$. We note that if $x \in A$ then $-x \notin A$ and if $y \in B$ then $-y \in B$.

Theorem 3 *Suppose there is a $GL(\ell)$-pair. Then there exists an Hadamard matrix of order $2\ell + 2$.*

Proof. The sequences are used to make two circulant matrices A and B of order ℓ. Then the following matrix is the required Hadamard matrix.

$$\left[\begin{array}{cc|ccc} - & - & + & \cdots & + \\ - & + & + & \cdots & + \\ \hline + & + & & & \\ \vdots & \vdots & & A & \\ + & + & & & \\ + & - & & & \\ \vdots & \vdots & & B^T & \\ + & - & & & \end{array}\right.\left.\begin{array}{ccc} + & \cdots & + \\ - & \cdots & - \\ \hline & & \\ & B & \\ & & \\ & & \\ & -A^T & \\ & & \end{array}\right]$$

Corollary 1 *Suppose that there are $2 - \{\ell; \frac{\ell+1}{2}, \frac{\ell+1}{2}; \frac{\ell+1}{2}\}$ SDS. Then there exists an Hadamard matrix of order $2\ell + 2$.*

Proof. The sequences are used to make two circulant matrices $\mathcal{A}$ and $\mathcal{B}$ of order ℓ. Now let J be the $\ell \times \ell$ matrix of all ones. Set $A = 2\mathcal{A} - J$ and $B = 2\mathcal{B} - J$. These are now used in the matrix of Theorem 3.

4 Existence of $GL(\ell)$–Pairs

$GL(\ell)$–pairs exist for the following lengths ℓ (the following sets indicated for ℓ are not necessarily disjoint), where:

- ℓ is a prime (see Section 3 this paper);
- $2\ell+1$ is a prime power (these arise from Szekeres difference sets, see for example, [GerSeb79]);
- $\ell = 2^k - 1$, $k \geq 2$ (two Galois sequences are a $GL(\ell)$–pair, see for example, [Schroeder84]);
- $\ell = p(p+2)$ where p and $p+2$ are both primes (two such sequences are a $GL(\ell)$–pair, see for example, [StanSprott58, Whiteman62]);
- $\ell = 49, 57$ (these have been found by a non–exhaustive computer–search that uses generalised cyclotomy and master–switch techniques, [GerSeb79], [GysSeb97]);
- $\ell = 3, 5, \ldots, 47$ (these have been found by exhaustive computer searches described herein);
- $\ell = 49,\ 51,\ 53$ and 55 (these have been found by partial computer searches described herein).

$GL(\ell)$–pairs do not exist for even lengths. The following lengths $\ell \leq 200$ are unresolved: 77, 85, 87, 91, 93, 115, 117, 121, 123, 129, 133, 145, 147, 159, 161, 169, 171, 175, 177, 185, 187 and 195.

5 Numerical Tools and Results

5.1 The PSD Test

We suppose that the set of numbers comprising sequences U and V are fixed and that only permutations of these sequences will be considered. Now every term in a PSD is non–negative. Hence if the sequences U and V are compatible, then no term in their PSDs can exceed the constant c in Theorem 2. That is,

$$|\mu_k|^2 + |\nu_k|^2 = c \Longrightarrow |\mu_k|^2 \leq c.$$

Equivalently, if any term of a sequence's PSD exceeds c, then the sequence cannot be a member of a compatible pair and so may be discarded from our search. This test can be generalised in a straightforward manner to any family of sequences over any alphabet that have constant periodic autocorrelation function. (Since, the nonperiodic autocorrelation function being constant implies that the periodic autocorrelation function is constant, the above test is also applicable for such candidate sequences.)

SDS parameters	ℓ	w	c	Number of sequences	Number passing PSD Test	% passing PSD Test
2-(21;6,10;6)	21	6	10	54,264	9,093	16.75%
	21	10	10	352,716	9,618	2.72%
2-(21;11,11;11)	21	10	11	352,716	25,494	7.22%
2-(25;9,9;6)	25	9	12	2,042,975	104,125	5.09%
2-(25;13,13;13)	25	13	13	5,200,300	189,000	3.63%
2-(31;15,10;10)	31	10	15	44,352,165	1,620,835	3.65%
	31	15	15	300,540,195	1,595,384	0.53%
2-(31;16,16;16)	31	16	16	300,540,195	4,358,104	1.45%

Table 1: Empirical Performance of PSD Test for Binary Sequences.

5.2 Empirical Performance of the PSD Test for Binary Sequences

Exhaustive searches over the space of all binary $0, 1$–sequences were performed for various lengths ℓ and weights w (number of ones) to see what fraction of sequences actually pass the PSD test. The constant c, the threshold for the PSD test, was determined by (4). The results are shown Table 1. It is evident that very substantial reductions in the number of candidate sequences can be realised through the use of the PSD test.

5.3 Application of the PSD Test to the Search for $GL(\ell)$–Pairs

Exhaustive searches for all $GL(\ell)$–pairs of length $\ell \leq 47$ were conducted, and incomplete searches for $49 \leq \ell \leq 55$. For reasons of efficiency, the computer programs dealt with sequences composed of 0 and 1 instead of ± 1. We also found it convenient to identify each decimation class with an *offset PSD component* such that the offsets of compatible classes would sum to zero. (E.g., offset PSDs can be obtained by subtracting the two terms on the right hand side of (4) from the PSDs of U and V, respectively. Then, among all the decimations of a given sequence U, we can select that decimation with the offset $|\mu_1|^2$ of greatest magnitude to be the representative of its decimation class, and we let the first component of its offset PSD be the *offset* of the decimation class.)

The exhaustive search algorithm was divided into three steps. In the first step, all decimation classes of length ℓ and weight $w = \frac{\ell+1}{2}$ are exhaustively generated, and each one that passes the PSD test is saved in a list. In the second step, the list is sorted by offset. In this manner, pairs of classes with equal and opposite offsets can

7742	3.747	4		7AC8	0.000	1		7AC8	0.000	1
7D48	2.956	4		7A98	-1.618	2		76C2	1.618	2
72B2	-3.783	4		76C2	1.618	2		7A98	-1.618	2
7D0C	3.783	4		79A8	-2.236	2		6EC2	2.236	2
7368	-2.956	4		6EC2	2.236	2		79A8	-2.236	2
6CB8	-3.913	4		734A	-2.827	4	check	7D48	2.956	4
6D38	-3.747	4	sort	7D48	2.956	4	compat.	7368	-2.956	4
7534	-3.445	4	$\longrightarrow$	7368	-2.956	4	$\longrightarrow$	7658	-2.956	4
7658	-2.956	4		7658	-2.956	4		7742	3.747	4
734A	-2.827	4		7534	-3.445	4		6D38	-3.747	4
7B0A	3.913	4		7742	3.747	4		7D0C	3.783	4
7AC8	0.000	1		6D38	-3.747	4		72B2	-3.783	4
7A98	-1.618	2		72B2	-3.783	4		7B0A	3.913	4
76C2	1.618	2		7D0C	3.783	4		6CB8	-3.913	4
6EC2	2.236	2		7B0A	3.913	4				
79A8	-2.236	2		6CB8	-3.913	4				

Table 2: Exhaustive Search Results for $\ell = 15$.

be quickly found, and the third step is to compute the autocorrelation functions of such pairs to confirm whether they are compatible or not.

The results from these three steps for $\ell = 15$ are illustrated in Table 2. Decimation classes are represented in hexadecimal ($0 = 0000, 1 = 0001, 2 = 0010, \ldots, \mathrm{F} = 1111$) with leading zeros ignored. Each decimation class is followed by its offset and the number of distinct decimations comprising the class. Decimation classes 6EC2 and 79A8 are actually members of the same class, so the total number of decimation classes generated was 15. In the three rightmost columns, each line with a positive offset followed by one or more lines with a negative offset represent compatible classes. Note that class 7D48 is compatible with two different classes, namely 7368 and 7658.

5.4 Exhaustive Search Results

The results from the exhaustive searches for $\ell \leq 47$ are shown in Table 3. N_D denotes the total number of decimation classes that were generated, N_P the number that passed the PSD test, and N_C the number that form a compatible pair with some other decimation class. In counting the total number of $GL(\ell)$–pairs that are formed, we follow the convention that any pair of sequences that can be transformed into another pair by exchanging the sequences, cyclically shifting or reversing either of the sequences, or decimating both by the same amount are considered equivalent. Thus, N_{GL} denotes the total number of inequivalent $GL(\ell)$–pairs, which is approximately equal to one half of N_C. N_r and N_s are analogous to N_C except that they count sequences instead of decimation classes. For N_r, two sequences are considered equivalent if one can be obtained from the other by a cyclic shift or reversal. For N_s, they are equivalent if and only if one can be obtained from the other by a cyclic shift. Since $\gcd(\ell, w) = 1$, all ℓ cyclic shifts of these sequences are distinct.

ℓ	w	N_D	N_P	N_C	N_{GL}	N_r	N_s
3	2	1	1	1	1	1	1
5	3	1	1	1	1	2	2
7	4	2	1	1	1	1	2
9	5	4	2	2	1	6	9
11	6	6	3	3	2	11	17
13	7	14	3	3	4	10	18
15	8	66	15	13	8	43	82
17	9	95	11	10	8	74	146
19	10	280	28	15	9	109	209
21	11	1,464	107	36	22	207	408
23	12	2,694	135	52	28	562	1,113
25	13	10,452	378	77	46	770	1,540
27	14	41,410	1,201	183	102	1,647	3,294
29	15	95,640	1,895	255	139	3,546	7,076
31	16	323,396	4,696	382	201	5,654	11,308
33	17	1,770,963	20,284	548	287	5,475	10,940
35	18	5,405,026	46,250	1,632	829	19,513	39,014
37	19	13,269,146	77,403	1,298	679	23,236	46,470
39	20	73,663,402	351,918	4,581	2,318	54,896	109,780
41	21	164,107,650	516,993	2,888	1,463	57,678	115,330
43	22	582,538,732	1,348,420	4,010	2,014	84,004	168,008
45	23	3,811,895,344	6,095,209	6,071	3,058	72,810	145,620
47	24	7,457,847,082	9,364,413	7,619	3,817	175,215	350,430

Table 3: Summary of Exhaustive Search Results.

The ratio between N_D and N_P in Table 3 shows that the effectiveness of the PSD test continues to increase with increasing ℓ. The table also illustrates just how quickly the number of inequivalent $GL(\ell)$-pairs grows with ℓ. It is clearly impractical to list all the $GL(\ell)$-pairs here. In lieu of that, we list just one pair for each $\ell \leq 55$ in Tables 4 and 5. We have attempted to list only pairs that are not produced by known methods of construction. The sequences for $\ell = 49, 51, 53$ and 55 were produced by partial searches that employed the same technique as the exhaustive searches. The complete list of inequivalent GL-pairs is available upon request from the authors.

Length	Sequences
3	++-
	++-
5	+++--
	++-+-
7	+++-+--
	+++-+--
9	++++-+---
	++-+-++--
11	++++-++----
	++-+-+-++--
13	+++-+++-+----
	+++-+--+-++--
15	+++++-+----++--
	+++--+-+-++--+-
17	++++-+++--++-----
	+++-+--++-+-+--+-
19	++-+++-+++-----+-+-
	++++--+--++-+-++---
21	++++++-+----+--++-+--
	+++--+-+-++--++-+---
23	+++++-+++-+----++--+---
	+++-+--+-++-++---+-+--
25	+++-++++-+-++--+-++------
	+++++---+-+--++--++-+-+--
27	+++++-+-+-++++--++---+-----
	++-++--++--+-++++---+-+--+-
29	++-+-++++++--+--++---+-+---+-
	+++++-++----+-+++--+-+--++---
31	++++++++--+-+-+----+-++--+-+---
	+++++---+++--++--++-+-+--+--+--
33	++++++-+-+--++++-++-+---+---+----
	+++-++--+++-+-+--+--++-+--++----
35	+++--+-++--+-+++++-+++---++------+-
	++-++++-+-+--+---+++---+--++-+-+--
37	++++++++-+-++--+-+---+--++--+-+-+----
	+++-++-+--+++-+----++++--++----+-++--

Table 4: Sample $GL(\ell)$–Pairs from Computer Searches - I.

Length	Sequences
39	+++--++++++-+--+++-+-+-+--++-+--+-- --- ++-+-++--+++-+++-----++++-+-++--+--+-- +--
41	++-+++-+++++-+--++-----++--++-+-+--- ---+- ++++++---++-+--++-+-+-+--++---++-++- ---+-
43	+++-++++--+--+--++++-++--+-+-++---+-- ----+-- ++-++++---++-+--+++-+-+--+++-+---+-+ +----+-
45	++++-++-+++--+-+++-+-++---+++-++---- -+-----+- ++-+-++-++++---+---++++---++--+--++ -+---+-+-
47	+++-+++++-+-++-++----++-+---+--++++- -----+---+- ++++-++-++---++---+-+--++-+++--+-+-- +-+++-+----
49	++++++++++--+--++++-----++--+-+-+-++ ---+----+---- ++-+++--+--+-+-++----+-+++---++-+--+ +--+-+-++--+-
51	++++--++--++--+-+++++-++++-+--++---- +-+---++----+-- ++++++-+-+-++---+-+++---+-+--++-+++- +--+-++-+-----
53	+++++-+-++++--+-++--++++-+-+-+-++ -+-----++---+---+--- ++++-++--+--++--++++--+----++--+-+++ +-++-+-+-++------
55	+++++-+++-++--+--+++-+-++++--+--++-+ -+--------+---+-+-- +++++----+++--+-+-+++-++--+-+--+--+-
	+--+++-+++---+----

Table 5: Sample $GL(\ell)$–Pairs from Computer Searches - II.

References

[Damgard90] I. Damgard, On the randomness of Legendre and Jacobi sequences, *CRYPTO'88*, Springer–Verlag, LNCS 403, 163–172, 1990.

[GerSeb79] A.V. Geramita and J. Seberry, *Orthogonal Designs: Quadratic Forms and Hadamard Matrices*, Marcel Dekker, New York – Basel, 1979.

[GysSeb97] M. Gysin and J. Seberry, An experimental search and new combinatorial designs via a generalisation of cyclotomy, *Journal of Combinatorial Mathematics and Combinatorial Computing*, forthcoming.

[Paterson98] K.G. Paterson, Binary sequence sets with favorable correlations from difference sets and MDS codes, *IEEE Transactions on Information Theory*, Vol. 44, 1, 172–180, 1998.

[PFTV89] W.H. Press, B.P. Flannery, S.A. Teukolsky and W.T. Vettering, *Numerical Recipes in Pascal: The Art of Scientific Computing*, Cambridge Univ Press, New York, 1989.

[Tretter76] S.A. Tretter, *Introduction to Discrete–time Signal Processing*, John Wiley & Sons, New York, 1976.

[Schroeder84] M.R. Schroeder, *Number Theory in Science and Communication*, Springer–Verlag, New York, 1984.

[Seberry73] J. Seberry Wallis, Some remarks on supplementary difference sets, *Colloquia Mathematica Societatis Janos Bolyai*, 10, 1503–1526, Hungary, 1973.

[SebYam92] J. Seberry and M. Yamada, Hadamard matrices, sequences and block designs, *Contemporary Design Theory – a Collection of Surveys*, eds. J. Dinitz and D.R. Stinson, John Wiley and Sons, New York, 431–560, 1992.

[StanSprott58] R.G. Stanton and D.A. Sprott, A family of difference sets, *Canadian Journal of Mathematics*, 10, 73–77, 1958.

[WSW72] W.D. Wallis, Anne Penfold Street and Jennifer Seberry Wallis, *Combinatorics : Room Squares, Sum-free Sets, Hadamard Matrices*, 292, Lecture Notes in Mathematics, Springer Verlag, Berlin–Heidelberg–New York, 1972.

[Whiteman62] A.L. Whiteman, A family of difference sets, *Illinois Journal of Mathematics*, 6, 107–121, 1962.

(Received 18/1/2000)