Signed Groups, Sequences, and the Asymptotic Existence of Hadamard Matrices

R. CRAIGEN*

Department of Mathematics and Computer Science, University of Lethbridge, Lethbridge, Alberta, Canada T1K 3M4

Communicated by Vera Pless
Received December 15, 1993

We use the newly developed theory of signed groups and some known sequences with zero autocorrelation to derive new results on the asymptotic existence of Hadamard matrices. New values of $t$ are obtained such that, for any odd number $p$, there exists an Hadamard matrix of order $2tp$. These include: $t = 2N$, where $N$ is the number of nonzero digits in the binary expansion of $p$, and $t = 4^\lceil \frac{1}{2} \log_2((p-1)/2) \rceil + 2$. Both numbers improve on all previous general results, but neither uses the full power of our method. We also discuss some of the implications of our method in terms of signed group Hadamard matrices and signed group weighing matrices. There exists a circulant signed group Hadamard matrix of every even order $n$, using a suitable signed group. This result stands in striking contrast to the known results for Hadamard matrices and complex Hadamard matrices, and the circulant Hadamard matrix conjecture. Signed group weighing matrices of even order $n$ always exist, with any specified weight $w \leq n$. © 1995 Academic Press, Inc.

1. INTRODUCTION

Let us begin by recalling two well-known conjectures regarding orthogonal matrices, which are known respectively as the Hadamard matrix [8] and complex Hadamard matrix [12] conjectures.

**CONJECTURE 1.** There is an Hadamard matrix of order $n > 2$ if and only if $n \equiv 0 \mod 4$.

**CONJECTURE 2.** There is a complex Hadamard matrix of order $n > 1$ if and only if $n$ is even.

It is easy to show the necessity of the condition given in each of these conjectures. For the last 17 years or so, the best general asymptotic result regarding the existence of Hadamard matrices has been the following.

* Supported by an NSERC Postdoctoral Fellowship. E-mail address: craigen@cs.uleth.ca.
Theorem 1 (Seberry [13]). If \( p > 3 \) is an integer, then there exists an Hadamard matrix of order \( 2^t p \), where \( t = \lfloor 2 \log_2 (p - 3) \rfloor \).

Since the order of Hadamard matrices can always be doubled, this gives Hadamard matrices of all orders \( 2^t p \), \( s \geq t \). The number actually obtained in [13] is somewhat smaller in special cases, but this is the general lower bound for \( s \). The Hadamard matrix conjecture asserts that \( t \) in the theorem can be replaced with 2. We shall make significant progress in this direction. We shall also discuss some surprising implications of our results in the context of orthogonal matrices whose entries are elements of signed groups.

Here are a few conventions for matrices. The support of a matrix is the set of positions where its entries are nonzero. A matrix is quasisymmetric if it has the same support as its transpose. Matrices are disjoint if they have disjoint support.

With regard to \((0, \pm 1, \pm i)\)-sequences, \((0, \pm 1)\)-sequences and \((\pm 1)\)-sequences, we adopt the following conventions. The length of the sequence \( A = (a_0, \ldots, a_{l-1}) \) is the number \( l \), except when zeros are allowed, in which case it may be any number \( \geq l \). To \( A \) we associate a formal (Laurent) polynomial, \( f_A(x) = \sum_{i=0}^{l-1} a_i x^i \). We define the conjugate of the sequence \( A \) to be \( A^* = (\bar{a}_{l-1}, \ldots, \bar{a}_0) \). We also define the polynomial \( f^*_A(x) = \sum_{i=0}^{l-1} \bar{a}_i x^{-i} = x^{l-1} f_A(x) \). A list, \( A_1, \ldots, A_n \), of sequences is said to have zero autocorrelation\(^1\) with weight \( w \) if

\[
\sum_{i=1}^{n} f_{A_i}(x) f^*_{A_i}(x) = w, \tag{1}
\]

with operations performed formally over \( \mathbb{Z}[x] \). They have zero periodic autocorrelation of period \( p \) (which is also the length of the sequence) and weight \( w \) if (1) holds modulo the ideal \( \langle x^p - 1 \rangle \). We note that, if sequences \( A_1, \ldots, A_n \) of length \( \leq p \) have zero periodic autocorrelation of period \( p \) with weight \( w \), then they form the first rows of circulant \( p \times p \) \((0, \pm 1, \pm i)\)-matrices \( M_1, \ldots, M_n \), such that \( M_1 M_1^* + \cdots + M_n M_n^* = wI \). Sequences with zero autocorrelation have zero periodic autocorrelation for any period, \( p \).

Golay sequences are two \((\pm 1)\)-sequences of length \( g \) with zero autocorrelation, and \( g \) is called a Golay number. Base sequences are four \((\pm 1)\)-sequences of lengths \( m, m, m+q, m+q \) having zero autocorrelation. Golay numbers \( g = 2^a 10^b 26^c \) are known for all \( a, b, c \geq 0 \), and base sequences of lengths \( m, m, m+1, m+1 \) are known for all \( m \leq 30 \) or \( m \) a Golay number [11]. Complex Golay sequences (introduced in [5]) are \((\pm 1, \pm i)\)-sequences of length \( g \), having zero autocorrelation, and \( g \) is

\(^1\) The autocorrelation of a list of sequences \( A_i \) is the sequence of coefficients of terms of the polynomial on the left side of (1) having positive degree.
called a complex Golay number. These are known for all \( g = 2^a 3^b 5^c 26^d \), \( a, b, c, d \geq 0, a \geq b + c - 1 \).

We say that a sequence of length \( p \) is quasisymmetric if the corresponding \( p \times p \) circulant matrix is quasisymmetric.\(^2\) Similarly, sequences of the same length are disjoint if the corresponding circulant matrices are disjoint.

This paper is a direct descendant of [3] and [6], so the reader would do well to become familiar with the terminology and methods therein, although we sketch here the necessary background on signed groups in order that it be self-contained.

A signed group of order \( n \) is a group of order \( 2n \) with a distinguished central element of order 2, which we write as \(-1\).

Signed groups may be identified by their presentation, which is similar to the presentation of groups. The group of quaternions (a group of order 8, but also a signed group of order 4) is traditionally presented, not as a group, but as a signed group, as follows:

\[
Q = \langle i, j : i^2 = j^2 = -1, ij = -ji \rangle.
\]

Other small signed groups of interest are the trivial signed group:

\[
T = \langle -1 \rangle
\]

(which is the cyclic group of order 2, but has order 1 as a signed group), the complex signed group:

\[
S_c = \langle i : i^2 = -1 \rangle
\]

(as a group, \( S_c \) is the cyclic group order 4), and the dihedral group of order 8:

\[
D = \langle i, j : i^2 = j^2 = 1, ij = -ji \rangle
\]

(a signed group of order 4, and also sometimes presented in this way). The most important signed groups to us are the direct analogue of the symmetric groups, namely for each \( m \), the signed group of \( m \times m \) signed permutation matrices, which we denote by \( SP_m \). Notice that \( SP_2 \cong D \).

A representation of degree \( m \) of a signed group \( S \) is a rule that maps the elements of \( S \) into the set of \( m \times m \) matrices in such a way that \(-1\) is mapped to \(-I\) and multiplication is preserved. Of primary interest in this paper are representations of signed groups as signed subgroups of \( SP_m \). These we call remreps (short for “real monomial representations”). Notice, for example, that \( S_c \) has a remrep of degree 2. Remreps have the important

\(^2\) Note that this differs, but not irreconcilably, from Yang’s usage [14].
property that multiplicative inversion in the signed group corresponds to transpose of the matrices representing it.

The analogue of the group ring for a signed group $S$ is the signed group ring, $\mathbb{Z}[S]$, which is the group ring, modulo the ideal $\langle 1_z - 1_S \rangle$—that is, the ring whose elements are formal sums $\sum_{z \in P} z \cdot s$, where all the coefficients $z_s$ are in $\mathbb{Z}$, $P$ is a complete set of representatives of cosets of $\langle -1 \rangle$ in $S$, $-1_z$ is identified with $-1_S$, and operations are otherwise extended formally from the multiplication in $S$ and the operations of $\mathbb{Z}$. Clearly, $\mathbb{Z}[S]$ contains isomorphic copies of $\mathbb{Z}$ (as a ring) and $S$ (as a signed group). There is a natural involution in $\mathbb{Z}[S]$, which we call conjugation, $x \rightarrow x^*$, obtained by linear extension of multiplicative inversion in $S$. The signed group ring associated with $S_c$ is the ring of Gaussian integers. Conjugation in this ring is the usual complex conjugation.

The reader may verify that a degree $m$ remrep of $S$ extends uniquely to a representation of $\mathbb{Z}[S]$ as $m \times m$ matrices in which conjugation corresponds to matrix transpose. We shall be concerned with matrices whose entries are in $\mathbb{Z}[S]$, and define the adjoint of a matrix $M = (m_{ij})$ to be its conjugate transpose, $M^* = (m_{ji}^*)$. Note that if $S = S_c$, the adjoint is the usual Hermitian adjoint. Accordingly, we say that $M$ is normal if $MM^* = M^*M$.

We are most interested in matrices whose nonzero entries are in a signed group, $S$ (i.e., $(0, S)$-matrices; $S$-matrices if they have no zero entries). Recall that a weighing matrix of order $n$ and weight $w$ is an $n \times n (0, \pm 1)$-matrix $W = W(n, w)$ such that $WW^T = wI$. An Hadamard matrix, $H = H(n)$, is an $n \times n (\pm 1)$-matrix satisfying $HH^T = nI$. Similarly, complex weighing matrices and complex Hadamard matrices are defined respectively as $n \times n (0, \pm 1, \pm i)$-matrices $W = CW(n, w)$ satisfying $WW^* = wI_n$, and $n \times n (\pm 1, \pm i)$-matrices $H = CH(n)$ satisfying $HH^* = nI$. We now generalize these structures to signed group weighing matrices and signed group Hadamard matrices, which we define respectively as $n \times n (0, S)$-matrices $W = SW(n, w, S)$ satisfying $WW^* = wI_n$, and $n \times n S$-matrices $H = SH(n, S)$ satisfying $HH^* = nI$.

Much of this paper will be devoted to the construction of signed group Hadamard matrices from sequences. We will show how Hadamard matrices may be constructed in turn from these and thereby obtain powerful new results on the asymptotic existence of Hadamard matrices.

2. A CONSTRUCTION FOR SIGNED GROUP HADAMARD MATRICES

We shall repeatedly use the following simple generalization of Lemma 11 of [3].
LEMMA 2. Let $A, B$ be normal, commuting, disjoint $(0, S)$-matrices of order $n$. If

$$C = \begin{pmatrix} A + B & A - B \\ A^* - B^* & -A^* - B^* \end{pmatrix},$$

then $CC^* = C^*C = 2I_2 \otimes (AA^* + BB^*)$. Moreover, if $A$ and $B$ are both quasisymmetric and $S$ has a remrep of degree $m$, then there is a $(0, S_{2m})$-matrix $D$ of order $n$, having the same support as $A + B$, such that $DD^* = D^*D = AA^* + BB^*$. Further, if $A$ and $B$ are both circulant, so is $D$.

Proof. The claim concerning $C$ may be verified directly. The matrix $D$ is obtained as follows: Reorder the rows and columns of $C$ so that the resulting matrix, $D_0$, is partitioned into $2 \times 2$ blocks whose entries are the $(i,j)$, $(i+n,j)$, $(i,j+n)$ and $(i+n,j+n)$ entries of $C$, $1 \leq i, j \leq n$. Each nonzero block of $D_0$ will have one of the forms

$$\begin{pmatrix} a & a \\ b & -b \end{pmatrix} \text{ or } \begin{pmatrix} a & -a \\ b & b \end{pmatrix}, \quad \text{where } a, b \in S.$$

Multiplying $D_0$ on the right by $\frac{1}{2} I_n \otimes \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$, we get a $(0, S)$-matrix $D_1$, whose nonzero $2 \times 2$ blocks have one of the forms

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \text{ or } \begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix}, \quad \text{where } a, b \in S,$$  \hspace{1cm} (2)

and such that $D_1 D_1^* = D_1^*D_1 = (AA^* + BB^*) \otimes I_2$. The $2 \times 2$ matrices of the form (2) comprise a signed group which has a remrep of degree $2m$ (obtained by replacing $0, a, b$ with the $m \times m$ matrices representing them). Replacing each block of $D_1$ with the element of $S_{2m}$ it thus represents gives $D$. If $A$ and $B$ are circulant, then $C$ consists of four circulant blocks, so $D_0$ and $D_1$ are block-circulant ($2 \times 2$ blocks) and consequently $D$ is circulant. 

THEOREM 3. Suppose $X_1, \ldots, X_n$ are disjoint, quasisymmetric sequences having zero periodic autocorrelation of period $q$ and weight $w$.

1. If these are all $(0, \pm 1)$-sequences, then there is a circulant $SW(q, w, S_{2^{q-1}})$.

2. If $X_1$, $X_2$ are $(0, \pm 1, \pm i)$-sequences and $X_3, \ldots, X_n$ are $(0, \pm 1)$-sequences, then there is a circulant $SW(q, w, S_{2^r})$.

Proof. We let $M_1, \ldots, M_n$ be the circulant matrices having first rows $X_1, \ldots, X_n$. The first item follows by iterating Lemma 2, $n - 1$ times: The first iteration uses $M_1$ and $M_2$ to obtain a circulant $(0, S_P)$-matrix $N_1$, the next uses $N_1$ and $M_3$ to obtain a circulant $(0, S_{4})$-matrix $N_2$, etc. At each
step, $N_i$ and $M_{i+2}$ are disjoint, normal circulant $(0, S)$-matrices. Since $M_{i+2}$ has real entries, they also commute, so Lemma 2 applies again. The desired matrix is $N_{n-1}$.

The second case is similar, except that the first iteration of Lemma 2 uses the complex circulant matrices $M_1$, $M_2$ to obtain a circulant $(0, S\mathbb{P}_4)$-matrix. □

Now if a signed group Hadamard matrix $H$ of order $q > 1$ is to exist, it is necessary that $q$ be even, a fact (Theorem 2.15 of [1]) which can be seen by observing that each $s \in S$ must appear as a term in the inner product of two rows of $H$ as many times as $-s$. We consider a number of ways to use known sequences with zero autocorrelation to get sequences of length $q = 2p$ with the desired properties.

If $U$ and $V$ are sequences of length $l \leq (p-1)/2$, and $V^*$ has the same support as $U$, then $a$ and $b$ may be chosen so that $a + b = p - l - 1$ and the quasisymmetric sequences $X_{uv} = (0_{a+1}, U, 0_{2b+1}, V, 0_a)$ and $X_v = (0_{b+1}, V, 0_{2a+1}, -U, 0_b)$ are disjoint. These have periodic autocorrelation equal to twice the periodic autocorrelation of the sequences $(U, 0_{2p-1})$ and $(V, 0_{2p-1})$.

Suppose now that $U_1, \ldots, U_t, V_1, \ldots, V_t$ are sequences having zero autocorrelation and weight $w$, with total length no more than $p - 1$, and $V_j^*$ is the same length and has the same support as $U_j$, $j = 1, \ldots, t$. Then we may perform the above construction for each $j$, varying the values of $a$ and $b$ so as to obtain $2t$ quasisymmetric, disjoint sequences of length $2p$ having zero periodic autocorrelation and weight $2w$. The easiest way of guaranteeing the correct relationship between each $U_j$ and $V_j$ is to require them to be $(\pm 1)$-sequences of the same length. Fortunately, sets of 2 and 4 $(\pm 1)$-sequences with zero autocorrelation are known to exist in abundance (see, for example [11, 14]). Complex Golay sequences [5] are also natural to use (i.e., for $X_1, X_2$ in part 2 of Theorem 3). In fact, we can use any number of $(\pm 1)$-sequences gathered into pairs of the same length, with at most two complex sequences of equal length, as long as we have zero autocorrelation and the total of all the lengths is less than or equal to $p - 1$.

Let us now consider how large the signed group must be in Theorem 3. The measure of the "size" of a signed group that we are most interested in is the degree of its smallest remrep. Our constructions give a signed subgroup of $S\mathbb{P}_2$, so we know that this number is at most $2^n$ ($2^{n-1}$ if only real sequences are used).

A most crude bound on $n$ is obtained using only Golay sequences of length $2^t$, which exist for all $t$. Let $p$ be an odd positive integer. Henceforth, let us write $N = N(p)$ for the number of nonzero binary digits of $p$. If the $j$th nonzero binary digit of $(p - 1)/2$ corresponds to $2^j$, we form sequences $X_{2j+1}, X_{2j+2}$ of length $2p$, using Golay sequences $U, V$ of length $2^j$ in the
above construction. We also use \( X_1 = (1, 0_{2^{p-1}}), \ X_2 = (0^p, 1, 0_{p-1}) \) (or we could use the single sequence \( (1, 0_{p-1}, i_1, 0_{p-1}) \)). Altogether this gives us \( 2N \) disjoint, quasisymmetric sequences with zero periodic autocorrelation, period \( 2p \) and weight \( 2p \). The following result now follows by Theorem 3.

**Theorem 4.** For any odd positive integer \( p \), there exists a circulant \( SH(2p, SP_{2^{2p-1}}) \).

This is interesting in light of conjectures 1 and 2, considering that neither conjecture is anywhere near being resolved, for signed group Hadamard matrices generalize both real and complex Hadamard matrices. In contrast to Theorem 3, we have established here a uniform bound (best possible, in fact) on the exponent of 2 necessary in the order of a signed group Hadamard matrix (although we do not restrict the size of the signed group to make this statement, we clearly have some control on it)!

That the signed group Hadamard matrices we construct are all circulant is interesting in light of the long-standing conjecture that there is no circulant Hadamard matrix of order \( >4 \) [9], and the difficulty of finding more than a handful of circulant complex Hadamard matrices [12]. Because of their strong algebraic structure it is likely that these matrices will be found to have applications involving the coding, transmission, storage and retrieval of information.

### 3. A Construction for Hadamard Matrices

Lemma 9 of [3] gives the connection between orthogonal matrices whose nonzero entries lie in a signed group and those whose nonzero entries are \( \pm 1 \), and it has the following immediate consequence.

**Theorem 5.** If there is a \( SH(n, S) \) and \( S \) has a remrep of degree \( m \), the order of an Hadamard matrix, then there is an Hadamard matrix of order \( mn \).

*Proof (Sketch).* Replace each entry \( s \) of the \( SH(n, S) \) with \( \pi(s) H \), where \( \pi \) is the remrep and \( H \) is an Hadamard matrix of order \( m \).

Using direct sum, we see that if \( S \) has a remrep of degree \( m \), it has a remrep of any degree \( mq, q \) a positive integer. Now \( SP_m \) has a remrep of degree \( m \) (i.e., the natural representation), and so also of any degree \( mq \). Using Theorems 3 and 5, we give here some consequences of the method of Section 2.
THEOREM 6. Suppose there are \((\pm 1)\)-sequences \(A_1, B_1, \ldots, A_t, B_t\) with zero autocorrelation, \(A_i, B_i\) both having length \(l_i\), \(i = 1, \ldots, t\), where \(\sum_{i=1}^{t} l_i = L\). Then Hadamard matrices exists in orders

1. \(4^t+1(2L + 1)\);
2. \(2 \cdot 4^t+1(2L + 3)\);
3. \(2 \cdot 4^t+1(2L + 5)\);
4. \(2 \cdot 4^t+1(2L + 2g + 1)\), where \(g\) is a complex Golay number.

Moreover,

5. if there is an Hadamard matrix of order \(2 \cdot 4^t q\), then there is an Hadamard matrix of order \(4^t+1(2L + 1) q\);
6. if there is an Hadamard matrix of order \(4^t+1 q\), then there are Hadamard matrices of order \(2 \cdot 4^t+1(2L + 3) q\) and \(2 \cdot 4^t+1(2L + 5) q\);
7. if there is an Hadamard matrix of order \(4^t+2 q\), then there is an Hadamard matrix of order \(2 \cdot 4^t+2(2L + 2g + 1) q\).

Proof (Sketch). Part 1 follows by applying Theorem 5 (using an Hadamard matrix of order \(2^{2t+1}\)) to the signed group Hadamard matrices obtained in part 1 of Theorem 3 from \(2t + 2\) sequences constructed as in Section 2. For part 4, we use the two complex Golay sequences, \(U, V\) to form complex sequences \(X_U\) and \(X_V\) similar to the real ones obtained in Section 2, giving \(2t + 4\) sequences to be used in part 2 of Theorem 3. For parts 2 and 3, we replace \((1, 0_{2L}, 0, 0_{2L})\) and \((0, 0_{2L}, 1, 0_{2L})\) with complex sequences

\[
(1, -i, 0_{2(L-1)}, 0, 0, 0_{2(L-1)}, 1), \quad (0, 0, 0_{2(L-1)}, 1, i, 1, 0_{2(L-1)}, 0),
\]

obtained from complex Golay sequences of lengths 3, and

\[
(i, -i, i, 0_{2(L-2)}, 0, 0, 0, 0, 0_{2(L-2)}, 1, 1),
\]

\[
(0, 0, 0, 0_{2(L-2)}, 1, i, i, 1, -i, 0_{2(L-2)}, 0, 0),
\]
similarly obtained from complex Golay sequences of length 5. Parts 5, 6, and 7 follow from Theorem 5, with \(m = 2 \cdot 4^t q\), \(4^t+1 q\) and \(4^t+2 q\) respectively, using the signed group Hadamard matrices obtained in Theorem 3.

Of course, we may replace 3 and 5 in the statement of the theorem with any odd complex Golay number—these just happen to be the only ones known at present.3

3 Complex Golay sequences of lengths 11 and 13 are now known.
Corollary 7. For any odd positive integer \( p \), there exists a (block-circulant) Hadamard matrix of order \( 2^N p \).

This may be viewed as a corollary to either Theorem 6 (using Golay sequences of lengths \( 2^i \)), or Theorem 4 (via Theorem 5). The construction for Theorem 4 does not even come close to using the full power now available to us, considering the wide variety of sequences known. As a bound on the exponent of 2, however, it provides a strict improvement on Theorem 1 whenever \( N(p) < \lfloor 2 \log_2(p - 3) \rfloor / 2 \), which is the case for all \( p > 5 \) except \( p = 11, 13, 23, 47 \) (in which case equality is attained) and \( p = 2^s - 1 \) for some \( s \) (in which case the exponent given in Theorem 1 is one less). On average, \( N(p) \) is about \( \frac{1}{2} \log_2(p) \), so the exponent we obtain is on average about half the best previous one.

The possibilities for applying Theorem 3 seem endless, and this method will be subject to continual refinement as more is understood regarding sequences. For now, we shall be content with an even more convincing demonstration of the power of our method, and the construction of a few Hadamard matrices of relatively small order in Section 5.

The following lemma (essentially Theorem 4 of [14]) will be helpful.

Lemma 8. If there are base sequences of lengths \( m, m, m + 1, m + 1 \) and \( n, n, n + 1, n + 1 \), then there are four \((\pm 1)\)-sequences of length \((2m + 1)(2n + 1)\), having zero autocorrelation. Consequently, there are also four such sequences of length \( 2^s(2m + 1)(2n + 1) \), \( s \geq 0 \). In particular, we may choose \( m \) and \( n \) to be any nonnegative integers up to 30, or any Golay number.

Theorem 9. If \( p \) is an odd positive integer, then there is an Hadamard matrix of order \( 2^t p \), where \( t = \lfloor \frac{1}{2} \log_2((p - 1)/2) \rfloor + 2 \).

Proof. Base sequences provide 4 \((\pm 1)\)-sequences with zero autocorrelation, the sum of whose lengths is twice any odd number up to \( 61(=2^6 - 3) \). Since 100 and 26 are Golay numbers, there are four sequences whose total length is \( 252(=4 \cdot 63) \). Since we can double the length of any such set of sequences, we have four sequences, the sum of whose lengths is \( 2^t q \) for any \( t > 0, q < 63 \), and \( t > 1, q = 63 \). In this way we associate 4 sequences with every nonzero digit of the base 64 expansion of \( (p - 1)/2 \), except when \( p \equiv 127 \mod 128 \). The sum of the lengths of these sequences will be \( p - 1 = 2L \), and there will be at most \( 4 \lfloor \frac{1}{6} \log_2((p - 1)/2) \rfloor \) sequences in the resulting list.

We now take care of the remaining case. If \( p = 127 \), the result is known. If \( p > 127 \), \( p \equiv 127 \mod 128 \), we argue that the last two digits of \( (p - 1)/2 \) in base 64 represent a number that is half the sum of the lengths of 8 \((\pm 1)\)-sequences with zero autocorrelation, as follows.
Write \((p - 1)/2 \equiv r \mod 64^2\), \(r = 64k + 63, 0 \leq k \leq 63\). Now as long as \(1 \leq k \leq 31\), Lemma 8 gives four sequences of length 33\(k\), and 63 - 2\(k\) is half the sum of the lengths of base sequences. This gives 8 sequences altogether, with total length \(4(33k) + 2(63 - 2k) = 2r\). On the other hand, if \(34 \leq k \leq 63\) or \(k = 32\), Lemma 8 gives four \((\pm 1)\)-sequences of length 33\((k - 1)\), and 129 - 2\(k\) is half the sum of the lengths of base sequences, and we have 8 sequences with total length \(4 \cdot 33(k - 1) + 2(129 - 2k) = 2r\).

There remain two cases: (a) \(k = 0, r = 63 = 52 + 10 + 1\)—half the sum of the lengths of 6 Golay sequences—and (b) \(k = 33, r = 2175 = 2080 + 64 + 31\)—half the sum of the lengths of 4 Golay sequences and 4 base sequences. This takes care of the exceptional cases, showing that for \(p \neq 127, L = (p - 1)/2\) is the sum of the lengths of at most \(4^\lceil \frac{1}{6} \log_2((p - 1)/2) \rceil (\pm 1)\)-sequences with zero autocorrelation. The result follows by an application of part 1 of Theorem 6.

4. SOME COMMENTS ABOUT ORTHOGONAL MATRICES OVER SIGNED GROUPS

Though the method of Theorem 9 lacks finesse, it gives an exponent \(t\) about \(1/3\) the size of that given in Theorem 1, when \(p\) large. There is a qualitative difference between the two results: in Theorem 1 the order of magnitude of \(2^t\) compares to \(p^2\), while in Theorem 9, it compares to \(p^{2/3}\). So for the first time, we have that the power of two is less significant than the odd factor in the order of Hadamard matrices.

Theorem 9 demonstrates that an Hadamard matrix of order \(2^t p\) exists with \(t \leq 10\) for \(p < 8000\) (Theorem 1 gives up to \(t = 25\) in this range) and with \(t \leq 14\) for \(p < 500000\) (Theorem 1 gives up to \(t = 37\)). We shall see in Section 5 that it is a simple matter to significantly improve even on Theorem 9 in these ranges with our method.

In [3], it was conjectured that for every even positive integer \(n\), there is a signed group \(S\) such that a \(SW(n, n - 1, S)\) exists. This conjecture can be proved by leaving out the sequence \((1, 0_{n - 1})\) in the method of Section 2. Again we have a bound on the size of \(S\), which is better by a factor of 2 than the bound obtained for \(SH(n, S)\). The signed group weighing matrices we obtain are circulant while, in contrast, ordinary \(W(n, n - 1)\) are never circulant unless \(n = 2\) [4]. There are some handy replication theorems [3] that give infinite classes of \(SW(N, N - 1, S)\) from these, which in turn give signed group Hadamard matrices \(SH(N, S')\), where if \(S\) has a remrep of degree \(m\), then \(S'\) has a remrep of degree \(2m\).

Moreover, simply by making our sequences long enough, we see that it is possible to obtain \(SW(n, w, S)\) for any even \(n\) and \(w \leq n\), where \(S\) is a suitable signed group (depending only on \(w\)). These are also circulant, and give block-circulant (ordinary) weighing matrices. Therefore, if we ignore
the size of the signed group involved, we have a best possible result for the existence of signed group weighing matrices in even orders: they always exists! What can be shown in odd orders remains to be seen. Such matters will be discussed further elsewhere.

5. SOME CALCULATIONS

Here we construct the Hadamard matrix of order $2^6 \cdot 13$ given in Corollary 7. Of course this matrix is not new, but it will serve as an example of manageable size.

Now $(13 - 1)/2 = 6$ has binary expansion 110. We therefore use Golay sequences $X = (111 \ldots)$, $Y = (11 - 1 \ldots)$ of length 4 and $U = (11)$, $V = (1 -)$ of length 2. As described in Section 2, these give disjoint, quasisymmetric sequences

$$X_1 = (1000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
order $4 \cdot 13$. Even an Hadamard matrix of order $8 \cdot 13$ would produce no better than $128 \cdot 13q$ by known methods, which can multiply the odd parts of the orders of two Hadamard matrices only by incurring a "penalty" in the exponent of 2, so that the new exponent is one less than the sum of the exponents of the original matrices. But with our method, we would still be able to multiply by $q$ with no penalty!

Now let us obtain some new Hadamard matrices. We see that $N(1319) = 6$. The stronger version of Seberry's bound [13] gave the best previous Hadamard matrix of order $2^7 \cdot 1319$, namely $t = 18$ ($t = 20$ is given by Theorem 1), and Theorem 7 effortlessly improves this by a factor of $2^6$, giving $2^{12} \cdot 1319$. Similarly, Theorem 9 gives $2^{10} \cdot 1319$. Now $1319 = 2 \cdot 659 + 1$, and $659 = 2 \cdot 329 + 1$. Since there are 4-complementary sequences of length $329 = 7 \cdot 47$ (these can be obtained using Lemma 8) and 1 is a Golay number, we can take $t = 3$ and $L = 659$ in part 1 of Theorem 6, giving an Hadamard matrix of order $2^{10} \cdot 1319$. Better yet: $1319 = 4 \cdot 329 + 3$, and so by doubling the length of the above complementary sequences, we can take $t = 2$ in part 2 of Theorem 6, further improving this to $2^7 \cdot 1319$.

Here is a construction that could have been included in [6], illustrating the utility of the multiplication in Theorem 5. The construction for Theorem 12 of [3] gives $SH(2(g+3), SP_4)$, where $g$ is a Golay number. Hence $SH(2 \cdot 419, SP_4)$ exists. Now there is an Hadamard matrix of order $4 \cdot 3 = 12$, and so by Theorem 5 there is an Hadamard matrix of order $2 \cdot 4 \cdot 3 \cdot 419 = 2^3 \cdot 1257$, which is new.

Table I lists a few new exponents resulting from the development of signed groups, comparing these to Theorem 1 and the best previously known exponent [10, 11].

\begin{table}
\centering
\begin{tabular}{|c|c|c|c|c|c|}
\hline
$p$ & $t$ from Theorem 1 & Best & Previous & (Base 2 $t$ from Theorem 4) & (Base 64 $t$ from Theorem 9) \\
\hline
419 & 17 & 4 & 3 & 10 & 10 \\
479 & 17 & 16 & 4 & 16 & 10 \\
491 & 17 & 15 & 5 & 14 & 10 \\
599 & 18 & 8 & 6 & 12 & 10 \\
653 & 18 & 4 & 3 & 10 & 10 \\
659 & 18 & 17 & 4 & 10 & 10 \\
739 & 19 & 16 & 6 & 12 & 10 \\
\hline
\end{tabular}
\caption{Exponents $t$ for Hadamard Matrices of Order $2^t p$, from Various Sources}
\end{table}

Table continued
### TABLE I (continued)

<table>
<thead>
<tr>
<th></th>
<th>839</th>
<th>1223</th>
<th>1257</th>
<th>1319</th>
<th>1439</th>
<th>1447</th>
<th>1499</th>
<th>1567</th>
<th>1571</th>
<th>1783</th>
<th>1913</th>
<th>1987</th>
<th>2033</th>
<th>2039</th>
<th>2063</th>
<th>2287</th>
<th>2293</th>
<th>2371</th>
<th>2671</th>
<th>2677</th>
<th>2687</th>
<th>2699</th>
<th>2679</th>
<th>2693</th>
<th>3119</th>
<th>3271</th>
<th>3295</th>
<th>3307</th>
<th>3343</th>
<th>3359</th>
<th>3371</th>
<th>3437</th>
<th>3539</th>
<th>3547</th>
<th>3571</th>
<th>3669</th>
<th>3719</th>
<th>3749</th>
<th>3907</th>
</tr>
</thead>
<tbody>
<tr>
<td>19</td>
<td>19</td>
<td>20</td>
<td>20</td>
<td>20</td>
<td>20</td>
<td>20</td>
<td>21</td>
<td>21</td>
<td>21</td>
<td>21</td>
<td>21</td>
<td>21</td>
<td>21</td>
<td>22</td>
<td>22</td>
<td>22</td>
<td>22</td>
<td>22</td>
<td>22</td>
<td>22</td>
<td>22</td>
<td>22</td>
<td>22</td>
<td>22</td>
<td>22</td>
<td>22</td>
<td>22</td>
<td>22</td>
<td>22</td>
<td>22</td>
<td>22</td>
<td>22</td>
<td>22</td>
<td>22</td>
<td>22</td>
<td>22</td>
<td>22</td>
<td>22</td>
<td>22</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>8</td>
<td>18</td>
<td>19</td>
<td>19</td>
<td>19</td>
<td>18</td>
<td>19</td>
<td>18</td>
<td>7</td>
<td>19</td>
<td>16</td>
<td>20</td>
<td>20</td>
<td>8</td>
<td>20</td>
<td>20</td>
<td>22</td>
<td>9</td>
<td>9</td>
<td>9</td>
<td>21</td>
<td>21</td>
<td>21</td>
<td>21</td>
<td>7</td>
<td>7</td>
<td>9</td>
<td>9</td>
<td>9</td>
<td>22</td>
<td>22</td>
<td>22</td>
<td>22</td>
<td>22</td>
<td>22</td>
<td>22</td>
<td>22</td>
<td>22</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>6</td>
<td>4</td>
<td>10</td>
<td>10</td>
<td>7</td>
<td>6</td>
<td>6</td>
<td>7</td>
<td>7</td>
<td>3</td>
<td>9</td>
<td>3</td>
<td>7</td>
<td>8</td>
<td>12</td>
<td>6</td>
<td>6</td>
<td>9</td>
<td>7</td>
<td>16</td>
<td>14</td>
<td>16</td>
<td>7</td>
<td>18</td>
<td>7</td>
<td>12</td>
<td>7</td>
<td>18</td>
<td>6</td>
<td>16</td>
<td>6</td>
<td>16</td>
<td>6</td>
<td>16</td>
<td>6</td>
<td>16</td>
<td>6</td>
<td>16</td>
</tr>
<tr>
<td>12</td>
<td>6</td>
<td>12</td>
<td>12</td>
<td>12</td>
<td>14</td>
<td>14</td>
<td>16</td>
<td>14</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>8</td>
<td>10</td>
<td>10</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>10</td>
<td>12</td>
<td>12</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
</tr>
</tbody>
</table>

### REFERENCES


