The Journal of Fourier Analysis and Applications

Volume 10, Issue 3, 2004

Lebesgue Constants for Hadamard Matrices

Don Hadwin, K.J. Harrison, and J.A. Ward

Communicated by Hans G. Feichtinger

ABSTRACT. There are many advantages in the use of Hadamard matrices in digital signal processing. However one possible disadvantage is the so-called overflow, as measured by the associated Lebesgue constants. We show that for certain classes of recursively generated Hadamard matrices, there are logarithmic upper bounds for these constants. On the other hand, for some Hadamard matrices the Lebesgue constants are of order $\sqrt{m}$. *These results have natural analogues in classical Fourier analysis.*

1. Introduction

Let E be an $m \times n$ *Hadamard matrix,* which for our purposes means its entries are all ± 1 and its rows are mutually orthogonal. The rows of E form a basis of $\mathbf{R}^n$ precisely when $m = n$, and in this case we say that E is a *full* Hadamard matrix. The orthogonal projection onto the span of the rows of E is the matrix $S = n^{-1}E^*E$, where E^* is the transpose of E. The norm of S as a linear operator on $\mathbf{R}^n$ equipped with the Euclidean norm is 1, since it is an orthogonal projection. However there are other norms for $\mathbf{R}^n$, and each of these determines an operator or matrix norm. In particular, if $\|x\|_\infty = \sup_{1\le i\le n} |x_i|$ denotes the supremum norm for $\mathbf{R}^n$, then the corresponding ∞-norm (or *gain*) of an $m \times n$ matrix $A = (a_{ij})$ is defined by

$$\|A\|_\infty = \sup\left\{\|Ax\|_\infty : x \in \mathbf{R}^n,\ \|x\|_\infty = 1\right\} = \sup_{1\le i\le m} \sum_{j=1}^{n} \left|a_{ij}\right| . \tag{1.1}$$

The *Lebesgue constant* of E is the ∞-norm of the projection operator S. We write $\mathcal{L}(E) = \|S\|_\infty$. Thus if $E = (e_{ij})$, then

$$\mathcal{L}(E) = n^{-1} \sup_{1\le i\le m} \sum_{j=1}^{n} \left| \sum_{k=1}^{m} e_{ki}e_{kj} \right| . \tag{1.2}$$

Math Subject Classifications. 15A60, 42A10, 94A99.
Keywords and Phrases. Lebesgue constant, Hadamard matrices.

ISSN 1069-5869 DOI: 10.1007/s00041-004-0929-0

Lebesgue constants of Hadamard matrices are invariant under various elementary transformations. In particular, it follows easily from (1.2) that

$$\mathcal{L}(P_1 D_1 E D_2 P_2) = \mathcal{L}(E) \ ,$$

where D_1 and D_2 are diagonal matrices with ± 1 diagonal entries and P_1 and P_2 are permutation matrices. Thus $\mathcal{L}(E)$ is unchanged by multiplying any row or column of E by -1, or by reordering the rows or columns of E.

'Row inflations' also leave Lebesgue constants invariant. That is, suppose that E is a Hadamard matrix, r is a positive integer and that $[E\ E\ \dots\ E]$ denotes the $1 \times r$ block matrix, each of whose entries is E. Then it is easy to verify that

$$\mathcal{L}(E) = \mathcal{L}\left([E\ E\ \dots\ E]\right) \ . \tag{1.3}$$

There are many applications of Hadamard matrices in digital signal processing [2, 7, 8]. For example, a signal x may be treated as a vector in $\mathbf{R}^n$ and 'encoded' by its Fourier coefficients with respect to some orthogonal basis. Using a Hadamard matrix E, the rows of E are the basis vectors, and the Fourier coefficients are obtained by matrix multiplication; they are (up to a scalar multiple) simply the entries of Ex. Furthermore, the fact that the entries of E are all ± 1 means that the entries in the product Ex can be evaluated simply as sums and differences of the entries of x. The product Sx is a partial sum of this Fourier expansion and can also be evaluated easily. It can be regarded as a 'partial reconstruction' of x. In data reduction this reconstruction is based on a relatively small subset (of size m) of the full set of size n Fourier coefficients. However, an undesirable side effect of this process is the so-called '*overflow.*' In many practical situations, for example in the quantized intensities of pixels of an image, there is a natural bound on the size of the components x_i, and we would like the components of the reconstruction Sx to satisfy the same bound. The Lebesgue constant is a measure of the extent to which this can fail. If the gain $\mathcal{L}(E) = 1$, (which rarely occurs for Hadamard matrices), then the components of Sx satisfy the same uniform bound as the components of the original signal x. On the other hand, if $\mathcal{L}(E) \gg 1$ then there are signals x for which the reconstruction Sx has components that greatly exceed the bound on the components of x. For this reason we study the behavior of the Lebesgue constants associated with various types of Hadamard matrices. In particular, we are interested in the growth rates of $\mathcal{L}(E_m)$ as m increases, where E_m denotes the matrix consisting of the first m rows of a given Hadamard matrix E.

There is a strong Fourier analysis background to this study. Suppose that $\left\{e^{(r)} : r \in \mathbf{Z}\right\}$ is the standard Fourier basis of $L^2(-\pi, \pi)$, (here $e^{(r)}(t) = e^{\mathrm{irt}}$). Then the classical Lebesgue constants are

$$\mathcal{L}_m = \frac{1}{2\pi} \int_{-\pi}^{\pi} \left| \frac{\sin(m + 1/2)t}{\sin(t/2)} \right| dt \ .$$

These are the ∞-norms of the projections onto the subspace of $L^2(-\pi, \pi)$ spanned by $\left\{e^{(r)} : |r| \leq m\right\}$, and it is known [5] that $\mathcal{L}_m = \frac{2}{\pi} \log m + O(1)$. Furthermore, by a deep result of McGehee, Pigno and Smith [6], the ∞-norm of the projections onto the subspace of $L^2(-\pi, \pi)$ spanned by any set of m characters $e^{(r)}$ is at least $c_1 \log m$, for some constant $c_1 > 0$.

On the other hand, some rearrangements of the standard Fourier basis allow larger lower bounds for the Lebesgue constants. For example, if $r_1, r_2, r_3, \dots$ is a lacunary

sequence of frequencies satisfying $r_{k+1} \geq \alpha r_k$ for some $\alpha > 1$, then [4]

$$\mathcal{L}_m = \frac{1}{2\pi} \int_{-\pi}^{\pi} \left| \sum_{k=1}^{m} e^{ir_k t} \right| dt \geq c_2 \sqrt{m} \,, \tag{1.4}$$

for some $c_2 > 0$. (In fact, there is a more general result of the form (1.4) in which the set of frequencies form a Sidon set, and the constant c_2 is related to the 'Sidon constant' of that set).

We shall establish discrete analogues for this behavior. In particular, we shall show that $\mathcal{L}(E_m)$ is bounded above by $c_3 \log m$ for a reasonably wide class of recursively generated Hadamard matrices E. On the other hand, there are Hadamard matrices E for which $\mathcal{L}(E_m)$ grows at least as fast as $c_4\sqrt{m}$. Some of these can be obtained as 'lacunary' submatrices of the standard recursively generated ones. We shall also give heuristic arguments that suggest that the $\sqrt{m}$ growth of $\mathcal{L}(E_m)$ is typical rather than the exception.

2. Slow Growth

In this section we show that there are classes of recursively generated Hadamard matrices E for which the associated Lebesgue constants $\mathcal{L}(E_m)$ grow slowly with m, that is, have logarithmic bounds.

2.1 Hadamard–Sylvester Matrices

Perhaps the most familiar Hadamard matrices are tensor powers of the 2×2 matrix $H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$. We call these the *Hadamard–Sylvester matrices*. Thus $H^{(1)} = H$, and for $k \geq 1$ $H^{(k+1)}$ is defined recursively by

$$H^{(k+1)} = H^{(k)} \otimes H = \begin{bmatrix} H^{(k)} & H^{(k)} \\ H^{(k)} & -H^{(k)} \end{bmatrix} . \tag{2.1}$$

So $H^{(2)} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$, and so on. Each $H^{(k)}$ is a full Hadamard matrix of size $2^k \times 2^k$.

There is a formula for the entries of $H^{(k)}$ [2]. If $H^{(k)} = (h_{ij}^{(k)})$, then

$$h_{ij}^{(k)} = (-1)^{\mathbf{i}\cdot\mathbf{j}} \tag{2.2}$$

where $\mathbf{i} = i_{k-1}i_{k-2}\ldots i_1 i_0$ and $\mathbf{j} = j_{k-1}j_{k-2}\ldots j_1 j_0$ are the binary expansions of the row and column numbers i and j, and where $\mathbf{i}\cdot\mathbf{j} = \sum_{u=0}^{k-1} i_u j_u$. (For this purpose the rows and columns are numbered from 0 to $2^k - 1$).

It is easy to verify that $\mathcal{L}(H^{(k)}) = 1$ for each $k \geq 1$. We now examine the Lebesgue constants of the submatrices $H_m^{(k)}$. First we note that the numbers $\mathcal{L}(H_m^{(k)})$ are independent of k. To see this suppose that $m \leq 2^{k-1}$. Then $H_m^{(k)} = \left[H_m^{(k-1)} : H_m^{(k-1)} \right]$ by (2.1), and so

by the concatenation property (1.3)

$$\mathcal{L}\left(H_m^{(k)}\right) = \mathcal{L}\left(H_m^{(k-1)}\right) . \tag{2.3}$$

It follows from (2.3) that $\mathcal{L}(H_m^{(k)}) = \mathcal{L}(H_m^{(k')})$ if $m \leq 2^k \leq 2^{k'}$, and we denote this common value by $\mathcal{L}(H_m)$.

The special nature of the Hadamard–Sylvester matrices provides a simple recursive formula for the Lebesgue constants $\mathcal{L}(H_m)$. In fact an argument based on (2.2) shows that the sequence $(\mathcal{L}(H_m))_{m\geq 1}$ satisfies the recurrence relations

$$\mathcal{L}\,(H_{2m}) = \mathcal{L}(H_m) \text{ and } \mathcal{L}\,(H_{2m+1}) = \frac{\mathcal{L}(H_m) + \mathcal{L}\,(H_{m+1}) + 1}{2} \text{ for } m \geq 1\,. \tag{2.4}$$

The behavior of the sequence $(\mathcal{L}(H_m))_{m\geq 1}$ can be seen in its graph, part of which appears in Figure 1. Loosely speaking, $\mathcal{L}(H_m)$ depends upon the number of sign changes in the binary expansion of m.

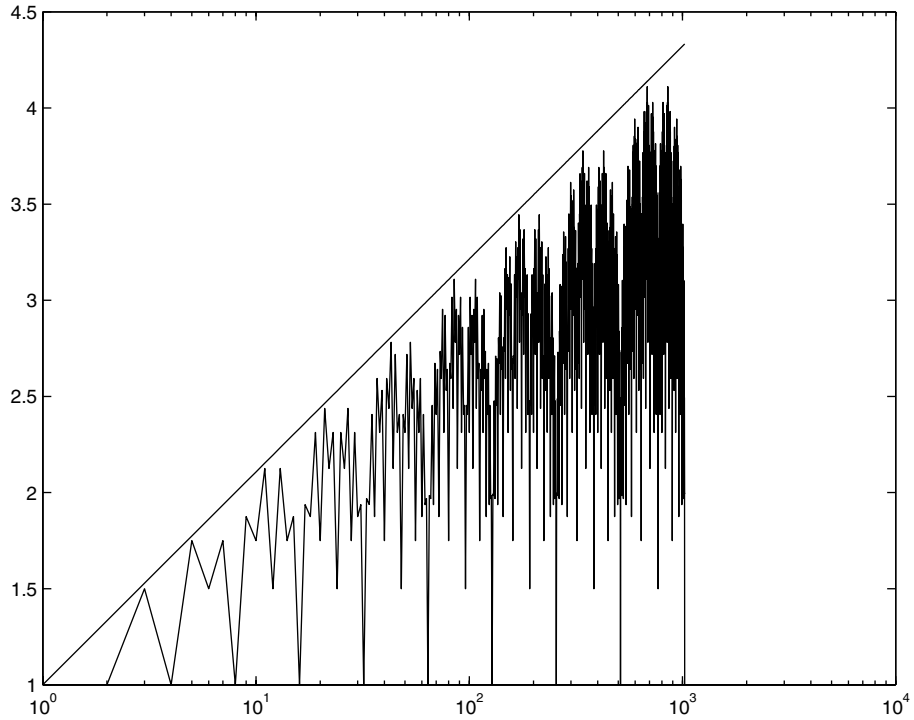

FIGURE 1

It follows from (2.4) that $\mathcal{L}(H_m) \geq 1$ for all m and $\mathcal{L}(H_m) = 1$ if and only if $m = 2^k$ for some non-negative integer k. Thus $\mathcal{L}(H_m)$ returns to its smallest value 1 at each integer power of 2. The largest value of $\mathcal{L}(H_m)$ in the interval $1 \leq m \leq 2^k$ occurs when $m \cong \frac{2}{3}2^k$ and $m \cong \frac{5}{6}2^k$. In fact, if Y_k denotes $\max_{1\leq m\leq 2^k} \mathcal{L}(H_m)$, then it can be shown using (2.4) that for each positive integer k,

$$Y_k = \frac{k}{3} + \frac{7}{9} + \frac{2}{9}\,(-2)^{-k} = \mathcal{L}(H_m), \text{ where } m = \frac{3}{4}2^k \pm \left(\frac{1}{12}2^k - \frac{1}{3}(-1)^k\right) . \tag{2.5}$$

The straight line in Figure 1 is the graph of $1 + \frac{1}{3}\log_2 m$. We can use (2.4) to show that $1 + \frac{1}{3}\log_2 m$ is indeed an upper bound for $\mathcal{L}(H_m)$. We state this result as our first theorem.

Theorem 1.

Let $H_m^{(k)}$ denote the $m \times 2^k$ matrix consisting of the first m rows of the k'th Hadamard–Sylvester matrix, where $1 \le m \le 2^k$. Then

$$\mathcal{L}\left(H_m^{(k)}\right) \le 1 + \frac{1}{3}\log_2 m \ .$$

Theorem 1 gives the sharpest bound for $\mathcal{L}(H_m)$ of the form $\alpha + \beta \log_2 m$. For if $\mathcal{L}(H_m) \le \alpha + \beta \log_2 m$ for all $m \ge 1$, then $\mathcal{L}(H_1) = 1$ implies that $\alpha \ge 1$ and (2.5) implies that $\beta \ge 1/3$.

2.2 A Class of Recursively Generated Hadamard Matrices

We give a recursive method for generating full Hadamard matrices including the standard Hadamard–Sylvester matrices $H^{(k)}$ as special cases. The construction was inspired by the recursive definition of the so-called PONS matrices as given in [1].

We start with a given full Hadamard matrix E of size $p \times p$, say. We write E in block column form

$$E = \begin{bmatrix} A_1 \\ A_2 \\ \vdots \\ A_q \end{bmatrix} , \tag{2.6}$$

where each A_r consists of p/q consecutive rows of E for some factor q of p. For $1 \le r \le q$ let $A_r^{(1)} = A_r$, and for each $k \ge 1$ let $A_r^{(k+1)}$ be the $p \times p$ block matrix given by

$$A_r^{(k+1)} = \left[e_{ij} A_{j+r-1}^{(k)} \right]_{i,j=1}^{p} , \tag{2.7}$$

where the subscript for $A^{(k)}$ in (2.7) is interpreted as $j + r - 1 \pmod q$. Finally we define for each $k \ge 1$

$$E^{(k)} = \left[A_1^{(k)} \ A_2^{(k)} \ \dots \ A_q^{(k)} \right]^* . \tag{2.8}$$

Example 1. If $E = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ and $q = 1$, then $E^{(k)} = H^{(k)}$, the k^{th} Hadamard–Sylvester matrix. However if we use the same starting matrix E and set $q = 2$, then $A_1 = A_1^{(1)} = \begin{bmatrix} 1 & 1 \end{bmatrix}$, $A_2 = A_2^{(1)} = \begin{bmatrix} 1 & -1 \end{bmatrix}$,

$$E^{(2)} = \begin{bmatrix} A_1^{(2)} \\ A_2^{(2)} \end{bmatrix} = \begin{bmatrix} A_1^{(1)} & A_2^{(1)} \\ A_1^{(1)} & -A_2^{(1)} \\ A_2^{(1)} & A_1^{(1)} \\ A_2^{(1)} & -A_1^{(1)} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & -1 & -1 & -1 \end{bmatrix} ,$$

and so on.

We can obtain logarithmic upper bounds for the Lebesgue constants associated with the recursively generated Hadamard matrices $E^{(k)}$, defined above. The proof appears in Section 4.

Theorem 2.
Let $E_m^{(k)}$ denote the $m \times p^k$ matrix consisting of the first m rows of the Hadamard matrix $E^{(k)}$ as defined by (2.8), where $1 \le m \le p^k$. Then

$$\mathcal{L}\left(E_m^{(k)}\right) \le \frac{p^2}{q}\left(1 + \log_p m\right) + \frac{p}{q} .$$

3. Rapid Growth

There are various ways of obtaining Hadamard matrices E whose Lebesgue constants $\mathcal{L}(E_m)$ grow rapidly, that is, faster than $c\sqrt{m}$. Perhaps the simplest of these is the following.

We shall say that an $m \times 2^m$ unimodular matrix is *column-complete* if its columns are all possible vectors of length m with ± 1 entries. It is easy to check that the rows of any such matrix are mutually orthogonal. We can show that the Lebesgue constant of such a matrix is of order $\sqrt{m}$.

Theorem 3.
If $B^{(m)}$ is a column-complete unimodular matrix of size $m \times 2^m$, then

$$\mathcal{L}\left(B^{(m)}\right)/\sqrt{m} \to \sqrt{2/\pi} \text{ as } m \to \infty .$$

Proof. Each entry of $B^{(m)*}B^{(m)}$ is a sum of the entries in one of the columns of $B^{(m)}$, and the rows of $B^{(m)*}B^{(m)}$ consist of all of these column sums, arranged in different orders. So the rows of $S = 2^{-m}B^{(m)*}B^{(m)}$ all have the same 1-norm, and $\mathcal{L}(B^{(m)})$ is the average of the absolute values of these column sums. That is,

$$\mathcal{L}\left(B^{(m)}\right) = 2^{-m}\sum_{j=1}^{2^m}\left|\sum_{i=1}^{m} b_{ij}\right| , \tag{3.1}$$

where b_{ij} is the (i, j) entry of $B^{(m)}$. The sum in (3.1) can be evaluated using the binomial theorem, but its form depends on whether m is even or odd. We can show that if m is even then

$$\mathcal{L}\left(B^{(m)}\right) = \mathcal{L}\left(B^{(m-1)}\right) = \frac{m(m)!}{((m/2)!)^2}2^{-m} = \sqrt{\frac{2m}{\pi}}e^{\theta_m/12m} ,$$

where $|\theta_m| < 1$, by Stirling's formula, and the theorem is proved. □

3.1 Lacunary Submatrices

We can show that drastic rearrangements of the rows of the Hadamard–Sylvester matrices can produce matrices whose Lebesgue constants grow rapidly. These rearrangements are natural analogues of the lacunary subsets in classical Fourier analysis.

Theorem 4.
Let $R_m^{(k)}$ denote the $m \times 2^k$ matrix consisting of rows $2^1, 2^2, \ldots, 2^m$ of $H^{(k)}$, where $m \leq k$. Then for m sufficiently large

$$\mathcal{L}\left(R_m^{(k)}\right) \approx \sqrt{2m/\pi}\ .$$

Proof. The recursive definition for $H^{(k)}$ can be used to show that $R_m^{(k)}$ is a row inflation of $R_m^{(m)}$ and that $R_m^{(m)}$ is column-complete. Now apply (1.3) and Theorem 3. □

We conjecture that similar results hold for lacunary submatrices of the matrices $E^{(k)}$ as defined in Section 2.2.

3.2 Random Bases

We now examine the expected behavior of the Lebesgue constant of a 'randomly generated' unimodular matrix, that is a matrix $E = (e_{ij})$ where the e_{ij} are independent random variables that take the values 1 and -1 with equal probability. We shall assume that $m^2 < n$, where m and n are the number of rows and columns of E, respectively. We define the Lebesgue constant of E in the same manner as before: $\mathcal{L}(E) = \|S\|_\infty$, where $S = n^{-1}E^*E$. The matrix S is unlikely to be an orthogonal projection, but we shall show that S is close to an orthogonal projection with high probability.

Theorem 5.
Let E be a randomly generated unimodular matrix of size $m \times n$, where $m < \alpha\sqrt{n}$ and $\alpha < 1$. Suppose also that $0 < \kappa < \sqrt{2/\pi}$ and that $\varepsilon > 0$. Then for all sufficiently large m,

$$\Pr\left(\mathcal{L}(E) > \kappa m^{1/2}\right) > 1 - \varepsilon\ . \tag{3.2}$$

Furthermore, if S' is the orthogonal projection onto the range of $S = n^{-1}E^*E$, then for all $\alpha' > \alpha$ and all sufficiently large m,

$$\Pr\left(\left\|S - S'\right\|_2 < \alpha'\right) > 1 - \varepsilon\ . \tag{3.3}$$

Proof. Write $S = (s_{ij})$ where $s_{ij} = n^{-1}\sum_{k=1}^m e_{ki}e_{kj}$. Then $s_{ii} = mn^{-1}$ for each i, and for each $i \neq j$, s_{ij} is a random variable with expected value $\mathfrak{E}(s_{ij}) = 0$ and variance $\mathfrak{Var}(s_{ij}) = mn^{-2}$. It follows from the binomial theorem and Stirling's formula that

$$\mathfrak{E}\left(|s_{ij}|\right) = \sqrt{2/\pi}\,e^{\theta/12m}m^{1/2}n^{-1} \text{ and } \mathfrak{Var}\left(|s_{ij}|\right) = \left(1 - \frac{2}{\pi}e^{\theta/6m}\right)mn^{-2} < mn^{-2}\ ,$$

for some θ (dependent on m) satisfying $|\theta| < 1$. So if $S^{(i)}$ denotes the i^{th} row of S, then

$$\begin{aligned}
\mathfrak{E}\left(\left\|S^{(i)}\right\|_1\right) &= mn^{-1} + \sqrt{2/\pi}\,e^{\theta/12m}m^{1/2}(n-1)n^{-1} \\
&> \sqrt{2/\pi}\,e^{\theta/12m}m^{1/2}, \text{ and} \\
\mathfrak{Var}\left(\left\|S^{(i)}\right\|_1\right) &< mn^{-1} < m^{-1}\ .
\end{aligned}$$

So by Chebychev's inequality, $\Pr\left(\left\|S^{(i)}\right\|_1 > \kappa m^{1/2}\right) > 1-\varepsilon$ for all sufficiently large m. Since $\mathcal{L}(E) = \|S\|_\infty = \sup_i \left\|S^{(i)}\right\|_1$, (3.2) follows.

Let $G = n^{-1}EE^* = (g_{ij})$. Then $g_{ij} = n^{-1}\sum_{k=1}^n e_{ik}e_{jk}$, and so $g_{ii} = 1$ for each i, and for $i \neq j$, g_{ij} is a random variable with expected value $\mathfrak{E}(g_{ij}) = 0$ and variance $\mathfrak{Var}(g_{ij}) = n^{-1}$. Let $\|I-G\|_{HS}$ denote the Hilbert–Schmidt norm of $I-G$. Then $\|I-G\|_{HS}^2 = \sum_{i\neq j} g_{ij}^2$, and

$$\begin{aligned}\mathfrak{E}\left(\|I-G\|_{HS}^2\right) &= m(m-1)n^{-1} < \alpha^2, \text{ and}\\ \mathfrak{Var}\left(\|I-G\|_{HS}^2\right) &= 4m(m-1)(n-1)n^{-3} < 4m^2n^{-2} < 4m^{-2}\,.\end{aligned}$$

So by Chebychev's inequality, $\Pr\left(\|I-G\|_{HS} < \alpha\right) > 1-\varepsilon$ for all sufficiently large m.

If $\|I-G\|_2 < 1$, then G^{-1} exists and has a positive square root $G^{-1/2}$. Let $F = G^{-1/2}E$, and let $S' = n^{-1}F^*F$. Then S' is an orthogonal projection with the same range as S. So $\|F\|_2 \leq n^{1/2}$, and

$$\left\|S'-S\right\|_2 = n^{-1}\left\|F^*(I-G)F\right\|_2 \leq \|I-G\|_2 \leq \|I-G\|_{HS}\ ,$$

and (3.3) follows. □

4. Proof of Theorem 2

In this section we outline the proof of the main result in Section 2.2. We shall need several lemmas, the first of which is a simple consequence of (1.1) and the triangle inequality.

Lemma 1.

Suppose that the matrix X has $m \times n$ block form: $X = \left[X_{ij}\right]$. Then

$$\|X\|_\infty \leq n \sup_{i,j} \left\|X_{ij}\right\|_\infty\ .$$

The second lemma ensures that the matrices $E^{(k)}$ are indeed Hadamard matrices.

Lemma 2.

Suppose that $A_r^{(k)}$ is as defined by (2.7). Then for $1 \leq r, s \leq q$ and $k \geq 1$,

$$p^{-k}A_r^{(k)}A_s^{(k)*} = \delta_{rs}I\ , \tag{4.1}$$

where I is an identity matrix.

Proof. The proof is by induction on k. From (2.6) EE^* has $q \times q$ block matrix form $(A_rA_s^*)_{r,s=1}^q$. But E is a Hadamard matrix and so $EE^* = pI$. So (4.1) holds for $k = 1$.

Now suppose that (4.1) holds for some $k \geq 1$. By (2.7) $A_r^{(k+1)}\ A_s^{(k+1)*}$ has $p \times p$ block matrix form $(B_{uv})_{u,v=1}^p$, where

$$B_{uv} = \sum_{w=1}^p e_{uw}e_{vw}A_{w+r-1}^{(k)}A_{w+s-1}^{(k)*} = \left(\sum_{w=1}^p e_{uw}e_{vw}\right)p^k\delta_{rs}I = p^{k+1}\delta_{rs}\delta_{uv}\ I\ ,$$

by the inductive hypothesis and the assumption that E is a Hadamard matrix. So $A_r^{(k+1)} A_s^{(k+1)*} = p^{k+1}\delta_{rs} I$, and since this establishes the inductive step, (4.1) holds for all $k \geq 1$. □

By (2.8) $E^{(k)} E^{(k)*}$ has $q \times q$ block matrix form $\left[A_r^{(k)} A_s^{(k)*}\right]_{r,s=1}^{q}$, and so by Lemma 2 $p^{-k} E^{(k)} E^{(k)*} = I$. It is clear from (2.7) and (2.8) that $E^{(k)}$ is unimodular, and so $E^{(k)}$ is a full Hadamard matrix.

Lemma 3.

For each positive integer $k \geq 1$ and $1 \leq r, s \leq q$,

$$p^{-k} \left\| A_r^{(k)*} A_s^{(k)} \right\|_\infty \leq p/q \ . \tag{4.2}$$

Proof. Again the proof is by induction on k. Since each A_s is a $p/q \times p$ unimodular matrix, $A_r^* A_s$ is a $p \times p$ matrix, each of whose entries is bounded in absolute value by p/q. Therefore $\left\| A_r^* A_s \right\|_\infty \leq p^2/q$. So (4.2) holds for $k = 1$.

Now suppose that (4.2) holds for some $k \geq 1$ (and all r and s). By (2.7) $A_r^{(k+1)*} A_s^{(k+1)}$ has $p \times p$ block matrix form $(C_{uv})_{u,v=1}^{p}$, where

$$C_{uv} = \left(\sum_{w=1}^{p} e_{wu} e_{wv} \right) A_{r+u-1}^{(k)*} A_{s+v-1}^{(k)} = p\delta_{uv} A_{r+u-1}^{(k)*} A_{s+u-1}^{(k)} \ ,$$

since E is a Hadamard matrix. So $A_r^{(k+1)*} A_s^{(k+1)}$ is a $p \times p$ block diagonal matrix with diagonal entries $pA_r^{(k)*} A_s^{(k)}$, $pA_{r+1}^{(k)*} A_{s+1}^{(k)}$, ..., $pA_{r+p-1}^{(k)*} A_{s+p-1}^{(k)}$, and hence

$$p^{-k-1} \left\| A_r^{(k+1)*} A_s^{(k+1)} \right\|_\infty = p^{-k} \sup_{1 \leq u \leq p} \left\| A_{r+u+1}^{(k)*} A_{s+u+1}^{(k)} \right\|_\infty \leq p/q \ ,$$

by the inductive hypothesis. So (4.2) holds for all $k \geq 1$. □

Lemma 4.

For each positive integer $k \geq 1$, $1 \leq r, s \leq q$, and $1 \leq m \leq p^k/q$,

$$p^{-k} \left\| A_r^{(k)*} P_m^{(k)} A_s^{(k)} \right\|_\infty \leq (k-1)p^2/q + p/q \ , \tag{4.3}$$

where $P_m^{(}k)$ is a diagonal matrix of size p^k/q times p^k/q, whose first m diagonal entries are all 1 and whose remaining diagonal entries are all 0.

Proof. Again the proof is by induction on k. By an argument similar to that used in Lemma 3, $\left\| A_r^* P_m^{(1)} A_s \right\|_\infty \leq p^2/q$. So (4.3) holds for $k = 1$.

Now suppose that (4.3) holds for some $k \geq 1$ (and all r, s and m). By (2.7)

$P_m^{(k+1)} A_s^{(k+1)}$ has $p \times p$ block matrix form:

$$\begin{bmatrix} e_{11}A_s^{(k)} & e_{12}A_{s+1}^{(k)} & \cdots & e_{1p}A_{s+p-1}^{(k)} \\ e_{21}A_s^{(k)} & e_{22}A_{s+1}^{(k)} & \cdots & e_{2p}A_{s+p-1}^{(k)} \\ \vdots & \vdots & \ddots & \vdots \\ e_{\mu 1}A_s^{(k)} & e_{\mu 2}A_{s+1}^{(k)} & \cdots & e_{\mu p}A_{s+p-1}^{(k)} \\ e_{\mu+1,1}P_\nu^{(k)}A_s^{(k)} & e_{\mu+1,2}P_\nu^{(k)}A_{s+1}^{(k)} & \cdots & e_{\mu+1,p}P_\nu^{(k)}A_{s+p-1}^{(k)} \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}, \tag{4.4}$$

where $m = \mu p^k/q + \nu$ and $1 \le \nu \le p^k/q$. So $A_r^{(k+1)*} P_m^{(k+1)} A_s^{(k+1)}$ has $p \times p$ block matrix form $(D_{uv})_{u,v=1}^p$, where

$$D_{uv} = \left(\sum_{t=1}^{\mu} e_{tu} e_{tv} \right) A_{r+u-1}^{(k)*} A_{s+v-1}^{(k)} + e_{\mu+1,u} e_{\mu+1,v} A_{r+u-1}^{(k)*} P_\nu^{(k)} A_{s+v-1}^{(k)} .$$

Therefore

$$\begin{aligned} \|D_{uv}\|_\infty &\le p \left\| A_{r+u-1}^{(k)*} A_{s+v-1}^{(k)} \right\|_\infty + \left\| A_{r+u-1}^{(k)*} P_\nu^{(k)} A_{s+v-1}^{(k)} \right\|_\infty \\ &\le p^{k+2}/q + p^k \left((k-1)p^2/q + p/q \right) \\ &= kp^{k+2}/q + p^{k+1}/q \end{aligned}$$

by Lemma 3 and the inductive hypothesis. So by Lemma 1

$$p^{-k-1} \left\| A_r^{(k+1)*} P_m^{(k+1)} A_s^{(k+1)} \right\|_\infty \le p^{-k} \sup_{u,v} \|D_{uv}\|_\infty \le kp^2/q + p/q .$$

So (4.3) holds for all $k \ge 1$. □

The next lemma gives a modification of inequality (4.3).

Lemma 5.

Suppose that $1 \le m \le p^{k'}/q$. Then for each $k \ge k'$ and $1 \le r, s \le q$,

$$p^{-k} \left\| A_r^{(k)*} P_m^{(k)} A_s^{(k)} \right\|_\infty \le \left(k' - 1 \right) p^2/q + p/q . \tag{4.5}$$

Proof. If $k = k'$, then (4.5) reduces to (4.3). So suppose that (4.5) holds for some $k \ge k'$. Then the $p \times p$ block matrix form (4.4) for $P_m^{(k+1)} A_s^{(k+1)}$ reduces to

$$\begin{bmatrix} e_{11}P_m^{(k)}A_s^{(k)} & e_{12}P_m^{(k)}A_{s+1}^{(k)} & \cdots & e_{1p}P_m^{(k)}A_{s+p-1}^{(k)} \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}.$$

So $A_r^{(k+1)*} P_m^{(k+1)} A_s^{(k+1)}$ has $p \times p$ block matrix form $\left[e_{1u} e_{1v} A_{r+u-1}^{(k)*} P_m^{(k)} A_{s+v-1}^{(k)} \right]_{u,v=1}^{p}$, and hence

$$\begin{aligned} p^{-k-1} \left\| A_r^{(k+1)*} P_m^{(k+1)} A_s^{(k+1)} \right\|_\infty &\leq p^{-k} \sup_{1 \leq u,v \leq p} \left\| A_{r+u-1}^{(k)*} P_m^{(k)} A_{s+v-1}^{(k)} \right\|_\infty \\ &\leq \left(k' - 1\right) p^2/q + p/q \end{aligned}$$

by Lemma 1 and the inductive hypothesis □

Lemma 6.

Suppose that $1 \leq m \leq p^k/q$ and $1 \leq r, s \leq q$. Then

$$p^{-k} \left\| A_r^{(k)*} P_m^{(k)} A_s^{(k)} \right\|_\infty \leq \frac{p^2}{q} \left(1 + \log_p m\right) + \frac{p}{q} .$$

Proof. Let $k' = \lceil \log_p mq \rceil$, the least integer greater than or equal to $\log_p mq$. Then $1 \leq m \leq p^{k'}/q$ and $k \geq k'$. So by Lemma 5

$$p^{-k} \left\| A_r^{(k)*} P_m^{(k)} A_s^{(k)} \right\|_\infty \leq \left(k' - 1\right) p^2/q + p/q .$$

But $k' - 1 \leq \log_p mq \leq 1 + \log_p m$ since $\log_p q < 1$. □

We can now complete the proof of Theorem 2 by finding the desired logarithmic bound for $\mathcal{L}(E_m^{(k)})$. Write $m = \mu p^k/q + \nu$, where $1 \leq \nu \leq p^k/q$. If $p^k/q \leq m$, then

$$E_m^{(k)} = \left(A_1^{(k)} \; A_2^{(k)} \; \ldots \; A_\mu^{(k)} \; P_\nu^{(k)} A_{\mu+1}^{(k)} \; 0 \; \ldots \; 0 \right)^T .$$

So by Lemmas 3 and 4,

$$\begin{aligned} \mathcal{L}\left(E_m^{(k)}\right) &= p^{-k} \left\| \sum_{t=1}^{\mu} A_t^{(k)*} A_t^{(k)} + A_{\mu+1}^{(k)*} P_\nu^{(k)} A_{\mu+1}^{(k)} \right\|_\infty \\ &\leq p^{-k} \sum_{t=1}^{\mu} \left\| A_t^{(k)*} A_t^{(k)} \right\|_\infty + p^{-k} \left\| A_{\mu+1}^{(k)*} P_\nu^{(k)} A_{\mu+1}^{(k)} \right\|_\infty \\ &\leq p^2/q + (k-1)p^2/q + p/q = kp^2/q + p/q \\ &\leq \left(1 + \log_p m\right) p^2/q + p/q . \end{aligned}$$

On the other hand, if $1 \leq m \leq p^k/q$, then

$$\begin{aligned} \mathcal{L}\left(E_m^{(k)}\right) &= p^{-k} \left\| A_1^{(k)*} P_m^{(k)} A_1^{(k)} \right\|_\infty \\ &\leq \left(1 + \log_p m\right) p^2/q + p/q \end{aligned}$$

by Lemma 6.

Acknowledgments

This work was inspired by a set of notes [3] on the mathematical properties of Prometheus orthonormal sequences (PONS) kindly given to the authors by Jim Byrnes.

References

[1] Byrnes, J.S. (1994). Quadrature mirror filters, low-crest factor arrays, functions achieving optimal uncertainty principle bounds, and complete orthonormal sequences: a unified approach, *Applied and Comp. Harm. Anal.,* **1**, 261–266.

[2] Davis, J.A. and Jedwab, J. (1999). Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed–Muller codes, *Trans. Inform. Theory,* **45**(7), 2397–2417.

[3] Byrnes, J.S. Mathematical characterizations of PONS constructions and properties, private communication.

[4] Edwards, R.E. (1967). *Fourier Series: A Modern Introduction,* Springer-Verlag.

[5] Hewitt, E. and Ross, K.A. (1970). *Abstract Harmonic Analysis,* Springer-Verlag, Berlin.

[6] McGehee, O.C., Pigno, L., and Smith, B. (1981). Hardy's inequality and the L^1 norm of exponential sums, *Ann. Math. (2),* **113**(3), 613–618.

[7] Silverstein, S.D. (1997). Application of orthogonal codes to the calibration of active phased array antennas for communication satellites, *IEEE Sign. Proc.,* **45**(1), 206–218.

[8] Yarlagadda, R. (1996). *Hadamard Matrix Analysis and Synthesis: with Applications to Communications and Signal/Image Processing,* Klewer.

Received April 16, 2002

Revision received December 25, 2002

University of New Hampshire

Murdoch University, Australia
e-mail: harrison@prodigal.murdoch.edu.au

Curtin University, Australia