Entropy and Hadamard matrices

2003 J. Phys. A: Math. Gen. 36 L109

(http://iopscience.iop.org/0305-4470/36/7/103)

INSTITUTE OF PHYSICS PUBLISHING JOURNAL OF PHYSICS A: MATHEMATICAL AND GENERAL

J. Phys. A: Math. Gen. **36** (2003) L109–L112 PII: S0305-4470(03)55295-7

LETTER TO THE EDITOR

Entropy and Hadamard matrices

H Gopalkrishna Gadiyar[1], **K M Sangeeta Maini**[1], **R Padma**[1] **and H S Sharatchandra**[2]

[1] AU-KBC Research Centre, M I T Campus, Anna University, Chromepet, Chennai 600 044, India
[2] Institute of Mathematical Sciences, C I T Campus, Taramani PO, Chennai 600 113, India

E-mail: gadiyar@au-kbc.org, sangeeta_maini@au-kbc.org, padma@au-kbc.org and sharat@imsc.res.in

Received 25 October 2002
Published 5 February 2003
Online at stacks.iop.org/JPhysA/36/L109

Abstract
The entropy of an orthogonal matrix is defined. It provides a new interpretation of Hadamard matrices as those that saturate the bound for entropy. It appears to be a useful Morse function on the group manifold. It has sharp maximum and other saddle points. The matrices corresponding to the maxima for three and five dimensions are presented. They are integer matrices (up to a rescaling).

PACS numbers: 02.90.+p, 02.10.Eb
Mathematics Subject Classification: 05B20, 15A15, 94A17

Hadamard's maximum determinant problem asks for $n \times n$ matrix h_n with elements of magnitude $\leqslant 1$ which has the maximum possible magnitude for the determinant. Hadamard's inequality is $|\det(h_n)| \leqslant n^{\frac{n}{2}}$. The equality is attained for some values of n, and the corresponding matrices are called Hadamard matrices H_n. They are orthogonal matrices up to a proportionality factor $\sqrt{n}$:

$$H_n H_n^T = n I_n \tag{1}$$

and have elements ± 1. The geometrical interpretation of the maximum determinant problem is to look for n vectors from the origin contained within the cubes $|x_i| \leqslant 1, i = 1, \ldots, n$ and forming a rectangular parallelopiped of maximum volume. In the case of Hadamard matrices, these vectors are a set of main diagonals, which obviously have the maximum possible lengths. Moreover they form an orthogonal set to provide the maximum volume. In other dimensions, it is not possible to have mutually orthogonal main diagonals. Nevertheless, we expect that the maximum determinant is from vectors which are 'close' to some main diagonals. This means that the entries of the matrix have magnitudes close to 1. Also we might expect a continuous set of matrices which have the maximum determinant because certain allowed changes in the vectors would increase their lengths and decrease the angles between them keeping the volume unchanged.

Hadamard matrices find natural applications in error-correcting codes [1] and provide 'biorthogonal' codes. There is extensive work on finding matrices with entries ± 1 which have maximum determinant. This is a subclass of the Hadamard's problem. There are also many generalizations and related problems. For example, Gritzmann *et al* [2] study the computationally difficult problem of finding the largest j-dimensional simplex in a given d-dimensional cube.

In this letter we use entropy to give a new criterion for the Hadamard matrix and obtain its generalization. We define the entropy of orthogonal matrices and Hadamard matrices (appropriately normalized) saturate the bound for the maximum of the entropy. The maxima (and other saddle points) of the entropy function have an intriguing structure and yield generalizations of Hadamard matrices. It appears that entropy is a very useful Morse function on the group manifold and not only the number [3] but also the location of the saddle points have interesting features.

Consider n random variables with a set of possible outcomes $i = 1, \ldots, n$ having probabilities p_i, $i = 1, \ldots, n$. We have $\sum_{i=1}^{n} p_i = 1$. The (Shannon) entropy is

$$H\{p_i\} = \sum_{n=1}^{n} p_i \ln \frac{1}{p_i}. \tag{2}$$

This has the minimum value zero for the case of certainty,

$$p_i = \begin{cases} 1 & \text{if} \quad i = j \text{ for some } j \\ 0 & \text{if} \quad i \neq j. \end{cases} \tag{3}$$

It has the maximum value $\ln n$ when all outcomes are equally likely,

$$p_i = \frac{1}{n} \qquad \forall i = 1, \ldots, n. \tag{4}$$

We now define entropy of an orthogonal matrix $O^i{}_j$, $i, j = 1, \ldots, n$. Here $O^i{}_j$ are real numbers with the constraint

$$\sum_{i=1}^{n} O^i{}_j O^i{}_k = \delta_{jk}. \tag{5}$$

In particular, the ith row of the matrix is a normalized vector for each $i = 1, \ldots, n$. We may associate probabilities $p_j^{(i)} = \left(O^i{}_j\right)^2$ with the ith row, as $\sum_{j=1}^{n} p_j^{(i)} = 1$, for each i. We define the (Shannon) entropy for the orthogonal matrix as the sum of the entropies of each row:

$$H\left\{O^i{}_j\right\} = -\sum_{i,j=1}^{n} \left(O^i{}_j\right)^2 \ln \left(O^i{}_j\right)^2. \tag{6}$$

The minimum value zero is attained by the identity matrix $O^i{}_j = \delta^i_j$ and related matrices obtained by interchanging rows or changing the signs of the elements. The entropy of the ith row can have the maximum value $\ln n$, which is attained when each element of the row is $\pm\frac{1}{\sqrt{n}}$. This gives the bound, $H\left\{O^i{}_j\right\} \leqslant n \ln n$. In general, the entropy of an orthogonal matrix cannot attain this bound because of the orthogonality constraint (5) which constrains $p_j^{(i)}$ for different rows. In fact the bound is obtained only by the Hadamard matrices (rescaled by $n^{-\frac{1}{2}}$). Thus we have a new criterion for the Hadamard matrices (appropriately normalized): those orthogonal matrices which saturate the bound for entropy.

Note that the entropy is large when each element is as close to $\pm\frac{1}{\sqrt{n}}$ as possible, i.e., to a main diagonal. Thus maximum entropy condition is similar to the maximum determinant condition of the Hadamard. Moreover, we find that the peaks of entropy are isolated and sharp in contrast to the determinant. Also, the matrices corresponding to the maxima have very interesting features even for those dimensions n for which Hadamard matrices do not exist. We have obtained matrices maximizing the entropy for $n = 3$ and 5 by numerical computation. For $n = 3$, the matrix is

$$\begin{bmatrix} -\frac{1}{3} & \frac{2}{3} & \frac{2}{3} \\ \frac{2}{3} & -\frac{1}{3} & \frac{2}{3} \\ \frac{2}{3} & \frac{2}{3} & -\frac{1}{3} \end{bmatrix}. \tag{7}$$

The matrix entries are all rational numbers and with a rescaling of each row by 3 we get an integer matrix. This was unexpected. For $n = 5$, the result is similar: the magnitudes of the elements in each row are $\frac{2}{5}$ repeated 4 times and a $\frac{3}{5}$. This set can be generalized for any n. The matrix with $-\frac{n-2}{n}$ along the diagonal and with each off-diagonal element as $\frac{2}{n}$ is orthogonal. Each row is normalized as a consequence of the identity

$$n^2 = (n-2)^2 + 2^2(n-1). \tag{8}$$

Also it is easily seen that any two rows are orthogonal to each other. For $n = 3$, 4 and 5, this family gives the maximum. Nonetheless, it is easy to argue that this cannot be the maximum for all n. For $n = 8$, the Hadamard matrix and not this family gives the maximum. For very large n the rows are close to one of the axes, and not to a main diagonal. Therefore the entropy is close to zero instead of being close to the bound $n \ln n$. We expect that different maxima emerge as n increases. It will be interesting to find the matrix corresponding to the maximum entropy for large n, but it is numerically difficult.

The picture that emerges is as follows. For each n, there are saddle points apart from maxima and minima. For example, for $n = 3$ there is a saddle point and the corresponding matrix is

$$\begin{bmatrix} \frac{1}{2} & \frac{1}{\sqrt{2}} & \frac{1}{2} \\ \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} \\ \frac{1}{2} & -\frac{1}{\sqrt{2}} & \frac{1}{2} \end{bmatrix}. \tag{9}$$

The entropy peaks quite sharply at all extrema. We expect that as n is varied there will be families of such extrema and there will be crossover among them.

Thus the entropy function has a rich set of sharp extrema. It appears to be a useful Morse function for the $O(n)$ group manifold. (It is possible to define the corresponding object for other group manifolds too.) Even the location of the saddle points, that is, the structure of the corresponding matrix is interesting. To our knowledge, entropy has not been applied as a Morse function in the past. (It has been applied for a classification of the Bernoulli shifts [4].)

The specific way in which the matrices (7), (9) solve the equations for the extrema is interesting. It turns out that they are simultaneously extrema of a class of entropy functions called Renyi entropy:

$$H_a\{O^i{}_j\} = \sum_{i,j} \left((O^i{}_j)^2\right)^a \tag{10}$$

where $a > 0$. We can recover the Shannon entropy from $O(\epsilon)$ terms when $a = 1 - \epsilon$. To obtain the equations for the extrema we use a Lagrange multiplier λ_{ij} symmetric in i and j for the constraint (5). The equations are

$$\left((O^i{}_j)^2\right)^{a-1} O^i{}_j = \frac{1}{a}\sum_k \lambda_{jk} O^i{}_k. \tag{11}$$

Using the orthogonality relation (5) we may rewrite this as

$$\sum_i \left((O^i{}_j)^2\right)^{a-1} O^i{}_j O^i{}_l = \frac{1}{a}\lambda_{jl}. \tag{12}$$

For $j = l$, this simply gives the value of λ_{jj}. The nontrivial equations are obtained by using $\lambda_{jl} = \lambda_{lj}$, $j \neq l$:

$$\sum_i \left((O^i{}_j)^2\right)^{a-1} O^i{}_j O^i{}_l = \sum_i \left((O^i{}_l)^2\right)^{a-1} O^i{}_l O^i{}_j \quad l \neq j. \tag{13}$$

We demonstrate how these nonlinear equations are satisfied by the maximum (7) for $n = 3$. Using the elements in the first and second rows, we have

$$\begin{aligned}&\left(\frac{1}{3}\right)^{2(a-1)}\left(-\frac{1}{3}\right)\left(\frac{2}{3}\right) + \left(\frac{2}{3}\right)^{2(a-1)}\left(\frac{2}{3}\right)\left(-\frac{1}{3}\right) + \left(\frac{2}{3}\right)^{2(a-1)}\left(\frac{2}{3}\right)\left(\frac{2}{3}\right)\\ &\qquad = \left(\frac{2}{3}\right)^{2(a-1)}\left(\frac{2}{3}\right)\left(-\frac{1}{3}\right) + \left(\frac{1}{3}\right)^{2(a-1)}\left(-\frac{1}{3}\right)\left(\frac{2}{3}\right) + \left(\frac{2}{3}\right)^{2(a-1)}\left(\frac{2}{3}\right)\left(\frac{2}{3}\right).\end{aligned} \tag{14}$$

We see that either $O^i{}_j = \pm O^i{}_l$ so that the contributions to the left-hand side and the right-hand side in equation (14) are the same; or else, $O^i{}_j = \pm O^{i'}{}_l$ for some i and i' so that again the contributions to the left-hand side and the right-hand side are the same.

In this letter we defined entropy of orthogonal matrices. We observed that it provides a new characterization of Hadamard matrices as those that saturate the bound for entropy. In dimensions where Hadamard matrices do not exist, entropy has sharp maxima (and other saddle points) in contrast with the determinant considered by Hadamard. We obtained matrices that maximize entropy in three and five dimensions. Surprisingly, they have rational entries. We argued that as n is varied there are families of maxima and saddle points which have interesting crossovers. It is challenging to find the maxima for large n (for non-Hadamard dimensions). We expect it will be close to Hadamard matrices in structure.

References

[1] McWilliams F J and Sloane N J A 1978 *The Theory of Error-Correcting Codes* (New York: Elsevier)

[2] Gritzmann P, Klee V and Larman D 1995 Largest j-simplices in n-polytopes *Disc. Comp. Geom.* **13** 477–515

[3] Bott R and Mather J 1968 *Topics in Topology and Differential Geometry (Battelle Rencontres, 1967, Lecture in Mathematics and Physics)* ed C M DeWitt and J A Wheeler (New York: Benjamin) pp 460–515

[4] Ornstein D S 1970 Bernoulli shifts with same entropy are isomorphic *Adv. Math.* **4** 337–52