

Hadamard Matrices

Instructor: Laszlo Babai

June 14, 2002

1 Introduction

Notation. $[n]$ denotes the set $\{1, 2, \dots, n\}$

Exercise 1.1 Let $4 \mid n$ and let $A_1, \dots, A_m \subset [n]$ such that for all $i \neq j$, $|A_i \cap A_j| = n/4$. Prove: $m \leq n - 1$. *Hint.* Use linear algebra.

Exercise 1.2 Prove that the inequality $m \leq n - 1$ in the preceding exercise is tight, i. e., for infinitely many values of n , set systems as described in the preceding exercise exist with $m = n - 1$. *Hint.* Does this problem belong in these notes?

Definition 1.3 A (± 1) -matrix is a matrix whose entries are 1 and -1 .

An $n \times n$ (± 1) -matrix is called an **Hadamard matrix** if the rows are orthogonal.

Remark. In Hadamard's name, the "H" and the final "d" are silent.

Exercise 1.4 Prove that an $n \times n$ (± 1) -matrix H is Hadamard $\Leftrightarrow H \cdot H^t = nI_n$, where I_n denotes the $n \times n$ identity matrix.

Definition 1.5 An $n \times n$ real matrix is *orthogonal* if $AA^t = I_n$.

Exercise 1.6 A real $n \times n$ matrix A is orthogonal $\Leftrightarrow (\forall x \in \mathbb{R}^n)(\|Ax\| = \|x\|)$, where $\|x\| = \sqrt{x \cdot x^t}$ denotes the Euclidean norm.

Exercise 1.7 Prove: if H is an $n \times n$ Hadamard matrix then $\frac{1}{\sqrt{n}}H$ is an orthogonal matrix.

Exercise 1.8 If H is an $n \times n$ Hadamard matrix then $(\forall x \in \mathbb{R}^n)(\|Hx\| = \sqrt{n}\|x\|)$.

Exercise 1.9 Prove that the columns of an Hadamard matrix are also orthogonal, i. e., $H^t \cdot H = nI_n$.

Exercise 1.10 Prove: all (complex) eigenvalues of an $n \times n$ Hadamard matrix have absolute value \sqrt{n} .

Exercise 1.11 Prove: if H is an $n \times n$ Hadamard matrix then $\det(H) = \pm n^{n/2}$.

Exercise 1.12 Prove: if A is an $n \times n$ (± 1) -matrix then $|\det(A)| \leq n^{n/2}$. Equality holds if and only if A is an Hadamard matrix. *Hint.* Prove Hadamard's Inequality: if A is an $n \times n$ real matrix then $|\det(A)| \leq N_1 \cdot \dots \cdot N_n$ where N_i is the Euclidean norm of the i^{th} row of A . Equality holds exactly when either a row is zero or the rows are orthogonal. Use the geometric meaning of the determinant (volume of the parallelepiped spanned by the rows).

Example 1.13 $S_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$,
 $S_{k+1} = \begin{bmatrix} S_k & S_k \\ S_k & -S_k \end{bmatrix} \quad (k \geq 1)$.

The matrix S_k is called the $2^k \times 2^k$ Sylvester matrix.

Exercise 1.14 Prove that S_k is an Hadamard matrix.

Exercise 1.15 Let $a_{v,w} = (-1)^{v \cdot w}$, where $v, w \in \mathbb{F}_2^k$. Prove that the $2^k \times 2^k$ matrix $(a_{v,w})$ is S_k (after suitable renumbering of the rows and columns).

Definition 1.16 The group $\mathbb{Z}_2^n = \mathbb{Z}_2 \times \dots \times \mathbb{Z}_2$ is called an **elementary Abelian 2-group**.

Remark. This group is the additive group of the n -dimensional vector space over \mathbb{F}_2 . (\mathbb{F}_2 is the field of two elements.) \mathbb{Z}_2^n is also the additive group of the field \mathbb{F}_{2^n} .

Exercise 1.17 Prove that the Sylvester matrix S_k is the character table of \mathbb{Z}_2^k .

Exercise 1.18 Let p be a prime number, $p \equiv -1 \pmod{4}$. Construct a $(p+1) \times (p+1)$ Hadamard matrix using the quadratic character of the field \mathbb{F}_p . *Hint.* Consider the $p \times p$ matrix (a_{ij}) where $a_{ij} = \left(\frac{i+j}{p}\right)$ (Legendre symbol). Modify this matrix by adding a row and column and suitably changing the zeros to ± 1 .

Exercise 1.19 Prove: if $\exists n \times n$ Hadamard matrix, then $n = 2$ or $4 \mid n$.

Exercise 1.20 Prove: if $\exists k \times k$ Hadamard matrix and $\exists l \times l$ Hadamard matrix, then $\exists kl \times kl$ Hadamard matrix.

Hint. Kronecker product.

Comment. The Sylvester matrices are Kronecker powers of S_1 : $S_k = S_1 \otimes \dots \otimes S_1$.

Conjecture 1.21 *If $4 \mid n$, then \exists an $n \times n$ Hadamard matrix.*

Comment. Let $\mathcal{H} = \{n \mid \exists n \times n \text{ Hadamard matrix}\}$ and let $h_n = |\mathcal{H} \cap [n]|$. If the conjecture is true, then $h_n = \Omega(n)$. But even this weak consequence of the conjecture remains unsolved.

OPEN PROBLEM 1.22 *Prove that $h_n \neq o(n)$.*

Exercise 1.23 Prove that $h_n = \Omega\left(\frac{n}{\log(n)}\right)$.

2 Discrepancy and Ramsey Theory for (± 1) -Matrices

Lemma 2.1 (Lindsey's Lemma) *Let $H = (h_{ij})$ be a Hadamard matrix. Let $S, T \subseteq [n]$ and $s = |S|$, $t = |T|$. Then*

$$\left| \sum_{i \in S} \sum_{j \in T} h_{ij} \right| \leq \sqrt{stn}.$$

Definition 2.2 We call the submatrix on the entries corresponding to $S \times T$ an $s \times t$ **rectangle** in H . We call the sum $\left| \sum_{i \in S} \sum_{j \in T} h_{ij} \right|$ the **discrepancy** of this rectangle.

Discrepancy measures the deviation from uniform distribution.

Exercise 2.3 Prove Lindsey's Lemma.

Hint. Let $v_S \in \{0, 1\}^n$ denote the incidence vector of $S \subseteq [n]$, i. e., the $(0, 1)$ -vector indicating membership in S . Observe that

$$\left| \sum_{i \in S} \sum_{j \in T} h_{ij} \right| = v_S H v_T^t.$$

Now use Exercise 1.8 and the Cauchy-Schwarz inequality:

$$(\forall a, b \in \mathbb{R}^n) (|a \cdot b| \leq \|a\| \cdot \|b\|).$$

Definition 2.4 A rectangle is **homogeneous** if all of its entries are equal.

Exercise 2.5 If H is an $n \times n$ Hadamard matrix, then H has no homogeneous rectangles of area $(= st)$ greater than n .

Exercise 2.6 (Erdős)

Prove: For all sufficiently large n , $\exists(n \times n)$ (± 1) matrices without homogeneous $t \times t$ rectangles such that $t \geq 1 + 2 \log_2 n$.

Hint. Use the Probabilistic Method. Flip a coin for each entry. Show that the probability that a random matrix is “bad” is less than 1. In fact it will be $o(1)$ (almost all matrices are “good”).

Exercise 2.7 Construct an explicit family of $(n \times n)$ (± 1) matrices A_n (for infinitely many values of n) such that A_n has no homogeneous $t \times t$ rectangles for $t > \sqrt{n}$.

OPEN PROBLEM 2.8 *Construct an explicit family of $(n \times n)$ (± 1) matrices A_n (for infinitely many values of n) such that A_n has no homogeneous $t \times t$ rectangles for $t > n^{0.49}$.*

3 Gale–Berlekamp Switching Game

Let $A = (a_{i,j})$ be a matrix with entries ± 1 . The first player sets the initial entries of A . Subsequently the second player may switch any row or column (multiply the row or column by -1) and repeat this operation any number of times. The second player’s “score” is the quantity $|\sum_{i,j \in [n]} a_{i,j}|$ which the second player wishes to maximize. The second player’s gain is the first player’s loss (zero-sum game), so the first player’s goal is to keep the second player’s score low.

Let $m(n)$ denote the score an optimal Player 2 can achieve against an optimal Player 1.

Exercise 3.1 Prove that $m(n) = \Theta(n^{3/2})$.

Hint 1. $m(n) = O(n^{3/2})$ requires Player 1 to be clever. Use an Hadamard matrix and Lindsey’s Lemma (Lemma 2.1). Warning: an $n \times n$ Hadamard matrix may not exist (but a slightly larger one will be just as good).

Hint 2. $m(n) = \Omega(n^{3/2})$). Player 2 needs a good strategy.

Let Player 2 flip a coin for each row to decide whether or not to switch that row. Subsequently, Player 2 should switch those columns whose sum is negative. Use the Central Limit Theorem for the analysis.