This paper deals with Hadamard matrices used as a method of error correction in transmitting information.

Note: this is an experimental text that may contain errors.

Hope I can help you with learning Quantum mechanics.

D. Kriesell page 1 of 9

Contents

Hadamard matrices	3
Blockcodes	4
Hadamard code	5
Entropy	7
Frequency picture	9

Hadamard matrices

The Hadamard transformation can be defined recursive.

$$\begin{split} H_0 &= 1 \\ H_1 &= \frac{1}{\sqrt{2}} \begin{pmatrix} H_0 & H_0 \\ H_0 & -H_0 \end{pmatrix} \equiv \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\ H_n &= H_1 \otimes H_{n-1} \end{split}$$

Note: n > 1.

The sequence of the first Hadamard matrices:

Note: The Hadamard matric can be viewed as a special discrete Fourier transform. More information you may find at https://en.wikipedia.org/wiki/Hadamard transform.

D. Kriesell page 3 of 9

An alternative way to calculate each element $H_m(k,n)$ is to decompose the index binary:

$$k = 2^{0} \cdot k_{0} + 2^{0} \cdot k_{1} + \dots + 2^{m-2} \cdot k_{m-2} + 2^{m-1} \cdot k_{m-1} = \sum_{i=0}^{m-1} 2^{i} k_{i}$$

$$n = 2^{0} \cdot n_{0} + 2^{0} \cdot n_{1} + \dots + 2^{m-2} \cdot n_{m-2} + 2^{m-1} \cdot n_{m-1} = \sum_{i=0}^{m-1} 2^{i} n_{i}$$

With this we can write:

$$H_m(k,n) = \frac{1}{2^{\left(\frac{m}{2}\right)}} \cdot (-1)^{\sum_j k_j n_j}$$

Note: $\sum_i k_i n_i$ is the inner product of the binary representation of k and n.

Example:

$$H_4(5,4) = \frac{1}{2^{\left(\frac{4}{2}\right)}} \cdot (-1)^{(101)\cdot(100)} = \frac{1}{\sqrt{2^4}} \cdot (-1)$$

Note: $H_4(0,0)$ is the upper left element of the matrix.

Blockcodes

Note: More information you may find at https://de.wikipedia.org/wiki/Blockcode.

We use an alphabet with k characters.

With this alphabet we define words, tuples of n elements:

A subset $C(n,k) \subset V(n,k)$ is called the valid words or a code C.

The Hamming distance of two words is the number of entries two words differ.

Example:

We use $V(4,4) = (0000) \dots (3333)$. This gives $4^4 = 256$ possible words.

The Hamming distance of the words (0123) and (1122) is two because the words differ in the first and last position.

The minimum distance between two words in a code is the smallest distance in a code \mathcal{C} .

If the minimum distance of a code $C=2\cdot e+1$ we call C an error detection code of grade $2\cdot e$, because the number of $2\cdot e$ errors or less don't give another valid element of code C. These errors are detectable after a transmission.

We call \mathcal{C} an e-error correcting code. If the number of errors occurring during a transmission is lower than or equal to e, then the distance of the erroneous word to the original word is lower than the distance to any other word in the code \mathcal{C} .

The Hamming weight is defined as the Hamming distance of each word to the zero-vector.

Example

We use $V(5,4) = (00000) \dots (33333)$.

D. Kriesell page 4 of 9

We use the code C := (00000), (11111), (22222), (33333), four valid words of length five each. These are the codes we know they are allowed.

The minimum distance between two words is $2 \cdot 2 + 1 = 5$.

The code detects 4 or less errors and can correct 2 or less errors.

Obviously, the code detects errors like: (00001), (00011), (00111), (01111)

The code would correct (00001), (00011) to (00000) because the distance to (00000) is smaller than the distance to (11111). If we get (00111), (01111) the code would correct this to (11111).

Hadamard code

We define a Hadamard matrix 4. This gives a 16×16 matrix.

We use the complementary matrix $-1 \cdot H_4$ too.

Each row of H_4 and $-H_4$ gives an element of code C.

We have $2 \cdot 2^4 = 32$ code words of length 16.

As the rows of the Hadamard matrix are orthogonal, two rows differ in $2^{4-1}=8$ positions. The Hamming distance of each code word is 8.

These properties usually are written as $[2^n, n+1, 2^{n-1}] code$, in our case $[2^4, 5, 2^3] code$.

The code detects up to 7 errors in transmission and is capable of correcting up to 3 errors.

The Hadamard matrix H_4 :

$$\frac{1}{1} \quad \frac{1}{1} \quad \frac{1}$$

We check the product of the Hadamard matrix with each allowed code word.

D. Kriesell page 5 of 9

The list of results:

We check what happens if we have a distorted signal.

We take the code word (111111111111111) and distort it in one position:

We check the product of the Hadamard matrix with this code word:

This holds with various distributions of +2 and -2 for all cases with a single distortion.

We take the code word (1111111111111111) and distort it in zero, one, two, ..., 16 positions and check the results multiplying it with the Hadamard matrix, omitting the factor $\frac{1}{\sqrt{3}}$:

D. Kriesell page 6 of 9

From this sample we see that we can correct up to three errors and restore the original code.

4 resp. 12 errors can clearly be detected as an erroneous transmission.

5 to 7, 9 to 11 and 13 to 15 errors are detectable but could mislead to a wrong error correction.

8 and 16 errors produce a syntactic correct but wrong code word.

Entropy

If we compare the identity matrix to the Hadamard matrix we see that the entropy of each vector of the identity matrix is at minimum whereas the entropy of the vectors of the Hadamard matrix is at maximum with exception of the first one.

We use the binary alphabet 1, -1.

We use equal probability: $P(1) = \frac{1}{2}$, $P(1) = \frac{1}{2}$

We get the information value of each bit 1, -1:

$$I(1) = -\left(\frac{1}{2} \cdot \log_2(\frac{1}{2})\right) = \frac{1}{2}$$

$$I(-1) = -\left(\frac{1}{2} \cdot \log_2(\frac{1}{2})\right) = \frac{1}{2}$$

We get the entropy of character 1:

$$H_1 = -P(1) \cdot log_2(P(1)) = \frac{1}{2}$$

The same holds for character 2.

The entropy of a message m is the expectation value E(m) of information value of all characters c contained in m:

$$H_m = E(m) = -\sum_{c \in m} P(c) \cdot log_2(P(c))$$

In our case we have a space of 2^{16} possible words. The transmitter choses 16 out of them, the rows or columns of the Hadamard matrix.

We name the possible words $w_1, w_2, ..., w_{16}$. They have equal probability $P(w_i) = \frac{1}{16}$.

All other words have probability zero.

D. Kriesell page 7 of 9

We name the entropy H_{s16} and get

$$H_{s16} = -\sum_{w_i} P(w_i) \cdot log_2(P(w_i)) = 16 \cdot \frac{1}{16} \cdot (-4) = 4$$

We calculate the entropy of one word used in the standard basis:

(100000000000000000)

We get the probabilities:

$$P(0) = \frac{15}{16}, P(1) = \frac{1}{16}$$

The entropy:

$$H_{std} = -\left(P(0) \cdot \log_2(P(0)) + P(1) \cdot \log_2(P(1))\right) =$$

$$-\left(\frac{15}{16} \cdot \log_2(\frac{15}{16}) + \frac{1}{16} \cdot \log_2(\frac{1}{16})\right) =$$

$$-\left(\frac{15}{16} \cdot (-0.0931) + \frac{1}{16} \cdot -4\right) = 0.3373$$

We calculate the entropy of the first word of the Hadamard basis, (111111111111111).

The entropy is zero.

We calculate the entropy of the second word of the Hadamard basis:

$$(1-11-11-11-11-11-11-11-1)$$

The probabilities for 1 and -1 each are 1/2.

We get the entropy

$$H_{had} = -\left(P(1) \cdot log_2\big(P(1)\big) + P(-1) \cdot log_2\big(P(-1)\big)\right) = 1$$

We get maximum entropy.

The mixture of minimum entropy in the first row and maximum in the other rows seems to be one reason for the capability of the Hadamard matrix to detect transmission errors.

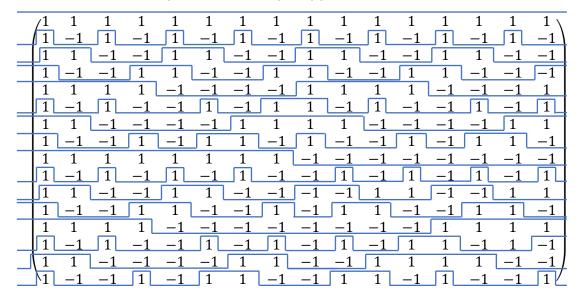
D. Kriesell page 8 of 9

Frequency picture

The identity matrix, presented in a frequency picture:

/1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0\	
/ o	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	
0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	
0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	
0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	
0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	
0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	
0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	
0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	
0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	
0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	
0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	
0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	
0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0 /	
/0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	

The Hadamard matrix, presented in a frequency picture:



D. Kriesell page 9 of 9