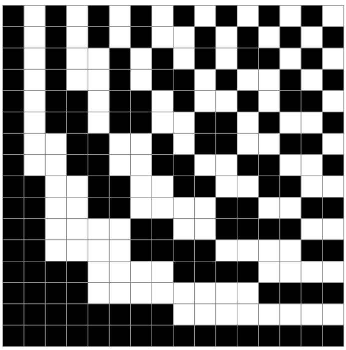
# Hadamard codes I – Hadamard matrices

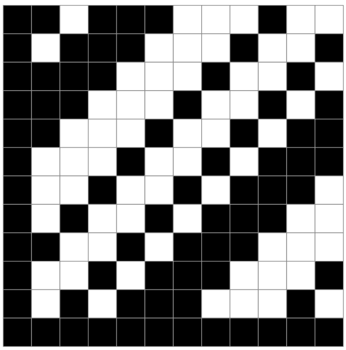
Monika Seidlová

An *Hadamard matrix* $H$ of order $n$ is a square $(n \times n)$ matrix with entries 1 or $-1$, such that $H \cdot H^T = nI_n$. It may equivalently be defined as a square matrix with entries 1 or $-1$, for which the scalar product of any pair of distinct rows or columns is 0. In other words, any two distinct rows or columns are orthogonal.

Hadamard matrices have been studied for almost 150 years. An English mathematician James Joseph Sylvester published their first examples in 1867. However, he did not view them as matrices, but as square grids made up of black and white cells. He called these grids *anallagmatic pavements.* In an anallagmatic pavement, when placing two rows or two columns side by side, half the adjacent cells are of the same colour and half differ. When interpreting the black cells as 1's and the white cells as $-1$'s in a square matrix, any two distinct rows or columns are orthogonal. Therefore, the matrix derived from an anallagmatic pavement is an Hadamard matrix. 26 years later in France, Jacques Hadamard was searching for the maximal determinant of square matrices with entries from the unit disc. He showed that the maximal determinant is $n^{n/2}$ and could be achieved by a matrix $H$ with entries $\pm 1$ if and only if $H \cdot H^T = nI_n$.

Examples of anallagmatic pavements:





There are several methods for construction of Hadamard matrices. Sylvester came up with a very simple one. He showed that if $H$ is an Hadamard matrix, then

$$\mathbf{H}' = \begin{pmatrix} H & H \\ H & -H \end{pmatrix}$$

is also an Hadamard matrix. Another method is Paley's construction. For an odd prime power $q$, such that $q \equiv 3 \bmod 4$, an Hadamard matrix of order $q+1$ can be constructed. If $q \equiv 1 \bmod 4$, then an Hadamard matrix of order $2(q+1)$ can be constructed. In both cases, a function, called the quadratic character, is used on elements of $F_q$ to attain the entries of a $(q \times q)$ matrix, which is further modified and expanded to construct the Paley Hadamard matrix.

An example of a matrix constructed by Sylvester's method:

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

Although not originally intended for these purposes, Hadamard matrices are now used in many applications. A binary error-correcting code with $2n$ code vectors and minimum distance $n/2$ can be obtained from an Hadamard matrix of order $n$. Such a code has maximal error-correcting capability for its codeword length. The matrices are also used to define Walsh functions, which are useful in signal modelling and transformation of information in image compression and image encoding. Furthermore, Hadamard matrices are used in screening designs and can help optimize weighing designs.

A big question about Hadamard matrices remains unanswered. There are orders, about which it is not known whether an Hadamard matrix exists or not. From Sylvester's construction we know that if an Hadamard matrix of order $n$ exists, then that of order $2n$ exists as well. The matrix of order 1 with the entry $\pm 1$ is an Hadamard matrix. Therefore, we know that for each $t$ natural an Hadamard matrix of the order $2^t$ exists. Hadamard contributed to the study of possible orders by proving that matrices bearing his name can exist only if $n$ is 1, 2 or a multiple of 4. This observation leads to the famous *Hadamard Conjecture*: if $n$ is 1, 2 or multiple of 4, does an Hadamard matrix of order $n$ always exist?