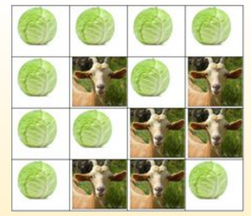
Hadamard Matrices

Raymond Jin, Matthew Drake, Vincent Ores, Evan Ward, John Grzegorczyk, Yuka Kimura
2020 Tennessee Governor's School for the Sciences and Engineering
Mathematics Course
Mentor Dr. Remus Nicoara and Assistant Mike Hanson



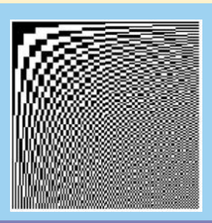
Hadamard Matrices

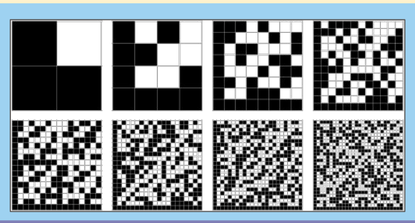
A Hadamard matrix *H* is an NxN matrix containing the values of ±1 such that each row of the matrix agrees with all other rows on exactly N/2, or half, of their positions. Another way to draw a Hadamard matrix is to use colored squares, with one color representing -1 and another representing 1.

Hadamard's Conjecture

Hadamard's Conjecture states that there exists a Hadamard matrix of order 4n for all natural numbers n.

While Sylvester's Construction proves the existence of Hadamard matrices of order 2^n, Paley's theorem guarantees the presence of a Hadamard matrix for all $m = 2^c (q^n + 1)$, where q is 0 or prime and c is a natural number such that m is divisible by 4. The existence of Hadamard matrices of the form 4p, where p is a prime number, is yet to be proven.



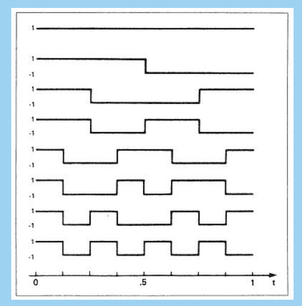


Walsh Functions

Walsh functions are periodic functions with entries of only 1 and -1. They are often used within Fourier analysis, which has applications in signal processing. In signal processing, Walsh functions are created through Walsh-Hadamard transforms (WHTs), a process in which a signal undergoes an orthogonal transformation that causes it to decompose into a set of orthogonal, rectangular waveforms with values -1 or +1.

In short, the way in which Hadamard matrices are connected to Walsh functions is the process in which Walsh functions are constructed. This creates a specific Hadamard matrix known as the Walsh matrix, pictured below on the left.

$$W(8) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \end{bmatrix},$$



Error Correction Coding

Error correction coding is the process of encrypting a message with redundant information so that errors can be more easily detected and fixed. Any NxN Hadamard matrix has corresponding 2N code words and a minimum distance of N/2. Based on these two properties, a Hadamard code can be generated from a Hadamard matrix. This code can then be used to encrypt the picture or message.

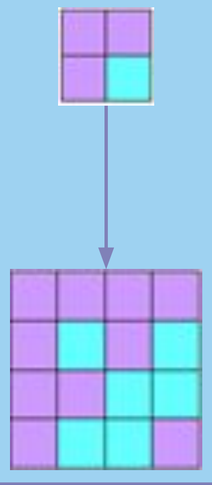
Two-dimensional Hadamard Error Correcting code utilizes "basis images," which are created through multiplying a column of a Hadamard matrix with a row of the same matrix. A NASA space mission used Hadamard matrices to decode pictures of Mars, Jupiter, Saturn, and Uranus.

Error Correction of a Goat Picture

Sylvester's Construction

Sylvester's Construction gives a partial proof for Hadamard's Conjecture, which states that if N is a multiple of 4, then there exists an NxN Hadamard matrix.

Sylvester's Construction proves that if there is a Hadamard matrix of size N, then there is a Hadamard matrix of size 2N, allowing for the construction of Hadamard matrices of sizes 2^k, where k is a non-negative integer.

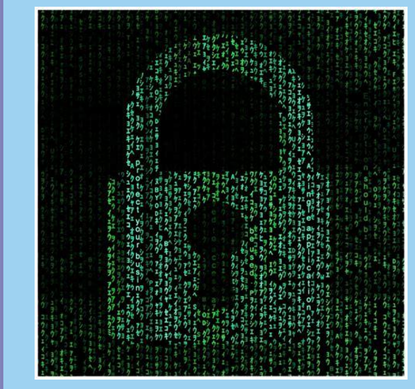


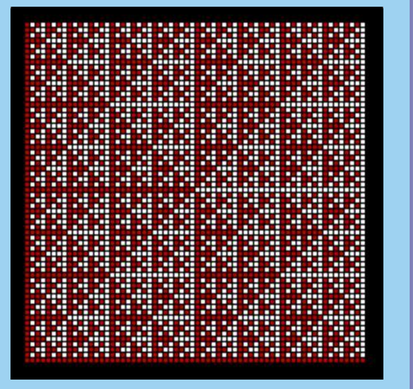
Historical Background

Sylvester was the first to investigate Hadamard matrices in 1867. He observed chess boards, on which patterns of colors in any two rows matched nowhere or everywhere. Jacques Hadamard later studied Hadamard matrices when looking for matrices with maximum determinants and was the first to construct Hadamard matrices of orders 12 and 20.

Encryption

Hadamard matrices are also often used in the construction of encryption schemes. One study showed that encryption schemes based on Hadamard matrices with circulant cores proved effective in defending against various types of cyber attacks, including "popular attacks, brute force, plaintext attacks, and ciphertext attacks" (Koukouvinos & Simos, 2013). This application is just one of many examples in which Hadamard matrices play an integral role in an essential aspect of our modern-day technology, which we often take for granted.





Logic Gates

Logic gates are the foundation of modern-day classical computers. They are simple operations or functions that take in bits as an input, change them in some way, then output them.

When broken down into its most basic form, all operations in a computer are done using logic gates. Some common examples of logic gates are the AND and OR gates.

Quantum Gates

Quantum gates are similar to logic gates, except they are done on qubits. One such gate is a Hadamard gate.

When a qubit passes through a Hadamard gate, it goes into a superposition state, which is what allows quantum computers to be so powerful compared to classical computers.