Paley Constructions of Hadamard Matrixes

Keith Wannamaker

January 23, 2025

Abstract

This document presents examples of constructing Hadamard matrixes using two methods attributed to Raymond Paley. In particular the illustrations include quadratic residue calculations from a Galois field for both the p^1 and p^k cases, polynomial division with remainder, and construction of the prerequisite Jacobsthal matrix for both cases.

The construction methods are implemented in Java at https://github.com/wannamak/hadamard/.

1 Background

A Hadamard matrix is an orthogonal matrix whose entries are -1 or 1, satisfying

$$\mathrm{HH}^T = n\mathrm{I}_n \tag{1}$$

For example, for n=4,

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{pmatrix} = 4 \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{2}$$

Properties:

- Any row (or column) may be exchanged with any row (or column).
- Any row (or column) may be negated.
- There are exactly n/2 differences between any two rows (or columns).

2 Choosing a construction

The Paley Construction methods for Hadamard matrices are based on a prime or a prime power. The resulting order is related to the prime or prime power by either:

$$n = p^k + 1 \tag{3}$$

or

$$n = 2(p^k + 1) \tag{4}$$

depending on the construction method.

Construction type one only works for the subset of odd primes where:

$$p \pmod 4 = 3 \tag{5}$$

Construction type two only works for the subset of odd primes where:

$$p \pmod 4 = 1 \tag{6}$$

Table 1 shows different alternatives for Paley construction of order ≤ 200. Notably absent are orders such as 16, which cannot be constructed by Paley's methods but which can be constructed by other techniques.

Table 1: Paley Constructions through order 200

Hadamard	Type I	Type II
order	p^k	p^k
4	3	
8	7	
12	11	5
20	19	3^2
24	23	
28	3^3	13
32	31	
36		17
44	43	
48	47	
52		5^2
60	59	29
68	67	
72	71	
76		37
80	79	
84	83	41
100		7^2
104	103	
108	107	53
124		61
128	127	
132	131	
140	139	
148		73
152	151	
164	163	3^4
168	167	
180	179	89
192	191	
196		97
200	199	

3 Quadratic residuals of primes

Paley made the connection between the pattern of quadratic residuals and the pattern of +1s in a Hadamard matrix.

To calculate quadratic residuals for odd n, for each integer $1..(n+1)/2$, examine the square modulo n. If non-zero, the square modulo n is a residual.

Table 2: Quadratic residues of selected odd primes

3	1
5	1, 4
7	1, 2, 4
9	1, 4, 7
11	1, 3, 4, 5, 9
13	1, 3, 4, 9, 10, 12
17	1, 2, 4, 8, 9, 13, 15, 16
19	1, 4, 5, 6, 7, 9, 11, 16, 17
21	1, 4, 7, 9, 15, 16, 18
23	1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18
25	1, 4, 6, 9, 11, 14, 16, 19, 21, 24
29	1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28
31	1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28
33	1, 3, 4, 9, 12, 15, 16, 22, 25, 27, 31
37	1, 3, 4, 7, 9, 10, 11, 12, 16, 21, 25, 26, 27, 28, 30, 33, 34, 36
41	1, 2, 4, 5, 8, 9, 10, 16, 18, 20, 21, 23, 25, 31, 32, 33, 36, 37, 39, 40
43	1, 4, 6, 9, 10, 11, 13, 14, 15, 16, 17, 21, 23, 24, 25, 31, 35, 36, 38, 40, 41
45	1, 4, 9, 10, 16, 19, 25, 31, 34, 36, 40
47	1, 2, 3, 4, 6, 7, 8, 9, 12, 14, 16, 17, 18, 21, 24, 25, 27, 28, 32, 34, 36, 37, 42
49	1, 2, 4, 8, 9, 11, 15, 16, 18, 22, 23, 25, 29, 30, 32, 36, 37, 39, 43, 44, 46
53	1, 4, 6, 7, 9, 10, 11, 13, 15, 16, 17, 24, 25, 28, 29, 36, 37, 38, 40, 42, 43, 44, 46, 47, 49, 52

4 Quadratic residuals of prime powers

For prime powers, the elements are derived from taking all possible combinations of coefficients from the elements of the prime itself. For example, for p=3, we consider elements 0, 1, and 2. So the elements of 3^2 are:

$$0 * x + 0, 0 * x + 1, 0 * x + 2, 1 * x + 0, 1 * x + 1, 1 * x + 2, 2 * x + 0, 2 * x + 1, 2 * x + 2 \tag{7}$$

or

$$0, 1, 2, x, x + 1, x + 2, 2x, 2x + 1, 2x + 2 \tag{8}$$

These are laid out as row and column labels, and the value of $row - column$ is calculated, modulo the minimum irreducible polynomial.

The quadratic residues for this field are:

$$1, 2, x, 2x \tag{9}$$

5 Paley Construction Type One

Construction type one assigns $row - column$ (mod p) to most cells, except the left column (all 1s), the top row (all 1s), and the remaining diagonal (all -1s):

$$\begin{pmatrix}1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\\ 1 & -1 & 6 & 5 & 4 & 3 & 2 & 1\\ 1 & 1 & -1 & 6 & 5 & 4 & 3 & 2\\ 1 & 2 & 1 & -1 & 6 & 5 & 4 & 3\\ 1 & 3 & 2 & 1 & -1 & 6 & 5 & 4\\ 1 & 4 & 3 & 2 & 1 & -1 & 6 & 5\\ 1 & 5 & 4 & 3 & 2 & 1 & -1 & 6\\ 1 & 6 & 5 & 4 & 3 & 2 & 1 & -1\end{pmatrix} \tag{10}$$

Now, replace all the $row - column \pmod{p}$ values with 1 if the number is a quadratic residual, else -1. For p = 7, residuals are (1, 2, 4), which yields the order 8 Hadamard matrix:

$$\begin{pmatrix}1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\\ 1 & - & - & - & 1 & - & 1 & 1\\ 1 & 1 & - & - & - & 1 & - & 1\\ 1 & 1 & 1 & - & - & - & 1 & -\\ 1 & - & 1 & 1 & - & - & - & 1\\ 1 & 1 & - & 1 & 1 & - & - & -\\ 1 & - & 1 & - & 1 & 1 & - & -\\ 1 & - & - & 1 & - & 1 & 1 & -\end{pmatrix} \tag{11}$$

6 Paley Construction Type Two

This method creates four matrices similar to type one, and concatenates them into the result.

Consider p = 5. We assign $row - column \pmod{p}$ values as before, with 1's in the top row, 1's in the left column, and 0's in the diagonal, with 0 being in the top left cell:

$$\begin{pmatrix}0 & 1 & 1 & 1 & 1 & 1\\ 1 & 0 & 4 & 3 & 2 & 1\\ 1 & 1 & 0 & 4 & 3 & 2\\ 1 & 2 & 1 & 0 & 4 & 3\\ 1 & 3 & 2 & 1 & 0 & 4\\ 1 & 4 & 3 & 2 & 1 & 0\end{pmatrix} \tag{12}$$

Now, replace all the $row - column \pmod{p}$ values with 1 if the number is a quadratic residual, else -1. For p = 5, residuals are (1, 4), which yields the matrix:

$$\begin{pmatrix}0 & 1 & 1 & 1 & 1 & 1\\ 1 & 0 & 1 & -1 & -1 & 1\\ 1 & 1 & 0 & 1 & -1 & -1\\ 1 & -1 & 1 & 0 & 1 & -1\\ 1 & -1 & -1 & 1 & 0 & 1\\ 1 & 1 & -1 & -1 & 1 & 0\end{pmatrix} \tag{13}$$

Now, assemble 4 copies of this matrix M in the following manner:

$$\begin{pmatrix}M + I & M - I\\ M - I & -M - I\end{pmatrix} \tag{14}$$

This constructs the following Hadamard matrix of order 12:

$$\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & - & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & - & - & 1 & 1 & - & 1 & - & - & 1 \\
1 & 1 & 1 & 1 & - & - & 1 & 1 & - & 1 & - & - \\
1 & - & 1 & 1 & 1 & - & 1 & - & 1 & - & 1 & - \\
1 & - & - & 1 & 1 & 1 & 1 & - & - & 1 & - & 1 \\
1 & 1 & - & - & 1 & 1 & 1 & 1 & - & - & 1 & - \\
- & 1 & 1 & 1 & 1 & 1 & - & - & - & - & - & - \\
1 & - & 1 & - & - & 1 & - & - & - & 1 & 1 & - \\
1 & 1 & - & 1 & - & - & - & - & - & - & 1 & 1 \\
1 & - & 1 & - & 1 & - & - & 1 & - & - & - & 1 \\
1 & - & - & 1 & - & 1 & - & 1 & 1 & - & - & - \\
1 & 1 & - & - & 1 & - & - & - & 1 & 1 & - & -
\end{pmatrix} \tag{15}$$

7 Code is King

Please see the Github repository above for code which implements these construction techniques. Requiem Aeternam for Mr. Paley who died tragically young in Banff National Park. His mind recognized an amazing pattern in the age before calculators and computers.