Paley Constructions of Hadamard Matrixes

Keith Wannamaker

January 12, 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

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

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