On Some Methods of Constructing Hadamard Matrices

Abdurzak M. Leghwel [1]

Abstract

There are two methods , often used to produce examples of algebraic and combinatorial structures . One of these methods begins with at least one example of the desired structure at hand and then constructs further structures of a like kind . We call such a construction method *recursive*. Another method (or methods) is to generate the desired structure simply after certain parameters regarding it have been specified . We shall call such a method of construction an *ab initio* method .

Hadamard matrices are algebraic structures in the sense that they form an important subclass of the class of matrices and hence must conform to all the algebraic rules obeyed by matrices under the usual operations of addition and multiplication . On the other hand , Hadamard matrices are combinatorial structures as well since the entries +1 and -1 of which the matrix consists must follow certain patterns . Thus one expects that one should be able to utilize both type of constructions methods , recursive and ab initio , to construct Hadamard matrices . This is indeed the case and in this paper we review some of these construction methods for Hadamard matrices .

In the second part we will introduce the concept of the Kronecker product and develop a recursive construction method for constructing Hadamard matrices based on it . Two important ab initio methods are discussed in the fourth part of this paper. These methods are due to Paley (1933) and is based on Galois fields . Hence some Galois field basics are presented in the third part also.

Keywords : Hadamard Matrix, Kronecker product, Galois fields.

1. Introduction

A (-1,1) - *matrix* is a matrix whose only entries are the numbers -1 or 1 . In this paper for the most part we will be interested in special (-1,1)-matrices called Hadamard matrices .

[1] Department of Mathematics, Faculty of Science, Alasmarya Islamic University, Zliten – Libya .

A *Hadamard matrix* of order n is an nxn (-1,1)- matrix H, satisfying $H'H = H'H = n I_n$, where H' denotes the transpose of H and I_n is the identity matrix of order n. If H is a Hadamard matrix, it follows from the definition that the set of row vectors of H, as well as, the set of column vectors of H form mutually orthogonal sets . The reader is referred to [6].

2. Construction of Hadamard Matrices Based on The Kronecker Product

In this part we present the construction of Hadamard matrices employing the Kronecker product . This construction is recursive and requires at least one Hadamard matrix at hand in order to utilize it . It is , therefore , most useful when employed in conjunction with some of the other techniques for constructing Hadamard matrices to be developed later . We begin by introducing the concept of the Kronecker product of matrices and some of its basic properties .

Definition : If $A = (a_{ij})$ is a pxq matrix and $B = (b_{ij})$ is a rxs matrix , then their *Kronecker product* $A \otimes B$ is the $prxqs$ matrix given by

Example 2.1 : If $A = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}_{2x2}$, $B = \begin{pmatrix} 2 & 4 \\ -5 & 3 \end{pmatrix}_{2x2}$,

then $$A \otimes B = \begin{pmatrix} 2 & 4 & 2 & 4 \\ -5 & 3 & -5 & 3 \\ 2 & 4 & -2 & -4 \\ -5 & 3 & 5 & -3 \end{pmatrix}_{4x4}$$

The basic properties concerning how the Kronecker product $\otimes$ relates to the matrix operations of addition , multiplication , scalar multiplication and transpose are given in the following theorem .

Theorem 2.1 : Let $A = (a_{ij})$ be a pxq matrix and $B = (b_{ij})$ be a rxs matrix. The Kronecker product $A \otimes B$ is a $prxqs$ matrix with the following properties :

i) $\alpha(A \otimes B) = (\alpha A) \otimes B = A \otimes (\alpha B)$ for any real number α ,

ii) $(A_1 + A_2) \otimes B = (A_1 \otimes B) + (A_2 \otimes B)$ and
$A \otimes (B_1 + B_2) = (A \otimes B_1) + (A \otimes B_2)$,

iii) $(A_1 \otimes B_1)(A_2 \otimes B_2) = A_1 A_2 \otimes B_1 B_2$, where the matrices A_i and B_i respectively are compatible for multiplication ,

iv) $(A \otimes B)' = A' \otimes B'$,

v) $(A \otimes B) \otimes C = A \otimes (B \otimes C)$ for any matrix C ,

vi) $(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}$, if A^{-1} and B^{-1} exist .

Proof : We will prove property (iv) , and we refer to a standard text in linear algebra for the rest .

Since

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1q}B \\ a_{21}B & a_{22}B & \cdots & a_{2q}B \\ \vdots & & & \\ a_{p1}B & a_{p2}B & \cdots & a_{pq}B \end{pmatrix}_{pr \times qs}, \quad (A \otimes B)' = \begin{pmatrix} a_{11}B' & a_{21}B' & \cdots & a_{p1}B' \\ a_{12}B' & a_{22}B' & \cdots & a_{p2}B' \\ \vdots & & & \\ a_{1q}B' & a_{2q}B' & \cdots & a_{pq}B' \end{pmatrix}_{qs \times pr} = A' \otimes B' .$$

□

The relationship between the determinant of the Kronecker product of square matrices and the determinant of individual matrices is given in the following :

Theorem 2.2 : For any two square matrices A of order m and B of order n, $\det(A \otimes B) = [\det(A)]^n [\det(B)]^m$.

Proof : We prove the theorem for the case when A has order $m = 2$.

Then $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}_{2x2}$ .If all $a_{ij} = 0$ then the theorem is clearly true . Hence , without loss of generality suppose that $a_{11} \neq 0$. Then

$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B \\ a_{21}B & a_{22}B \end{pmatrix}$. Further , we may also assume without loss of generality that $\det(B) \neq 0$. Then by [6, Theorem 3.1] ,

$\det(A \otimes B) = [\det(a_{11}B)]\,[\det(a_{22}B - a_{21}B(a_{11}B)^{-1}a_{12}B)]$

$= [\det(a_{11}B)][\det(a_{22}B - a_{21}a_{11}^{-1}a_{12}B)]$

$= \det[a_{11}B(a_{22}B - a_{21}a_{11}^{-1}a_{12}B)]$

$= \det[(a_{11}a_{22} - a_{21}a_{12})B^2] = (a_{11}a_{22} - a_{21}a_{12})^n \det(B^2)$

$= \det[A]^n \det[B^2] = [\det(A)]^n [\det(B)]^2$ and the theorem is proved for the case $m = 2$. □

From the viewpoint of Hadamard matrices , the properties of the Kronecker product immediately imply the following result :

Theorem 2.3 : If H_1 and H_2 are Hadamard matrices of orders n_1 and n_2 respectively , then $H_1 \otimes H_2$ is a Hadamard matrix of order $n_1 n_2$.

Proof : Let H_1 and H_2 be a Hadamard matrices of orders n_1 and n_2 respectively . Then

$(H_1 \otimes H_2)(H_1 \otimes H_2)' = (H_1 \otimes H_2)(H_{1'} \otimes H_{2'}) = H_1 H_{1'} \otimes H_2 H_{2'}$

$= n_1 I_{n_1} \otimes n_2 I_{n_2} = n_1 n_2 I_{n_1 n_2}$. □

Corollary 2.1. : Since there is a Hadamard matrix of order 2 , namely $H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, then there are Hadamard matrices of order 2^n for every positive integer n.

Proof : $H_{2^n} = H_2 \otimes H_2 \otimes \ldots \otimes H_2$, the Kronecker product of H_2 with itself extended over n factors gives the desired Hadamard matrix of order 2^n. □

Corollary 2.2 : If H is a Hadamard matrix of order k, for some positive integer k then there is a Hadamard matrix of order $2^n k$ for every positive integer n.

Proof : Let $H_1 = H \otimes H_{2^n}$, where H is a Hadamard matrix of order k, and H_{2^n} is the Hadamard matrix of order 2^n given in Corollary 2.1 . Then by Theorem 2.3, H_1 is a Hadamard matrix of order $2^n k$. □

Example 2.2 : Let H_2 be the normalized Hadamard matrix of order 2 . The matrix

$H_4 = H_2 \otimes H_2 = \begin{pmatrix} + & + & + & + \\ + & - & + & - \\ + & + & - & - \\ + & - & - & + \end{pmatrix}_{4x4}$ is a Hadamard matrix of order 4 .

By Theorem 2.3, we conclude that $H_{64} = H_4 \otimes H_4 \otimes H_4$ is a Hadamard matrix of order 64 .

Theorem 2.3 will be more helpful when we apply it to Hadamard matrices constructed by other methods . We discuss some of these other methods below .

3. Some Galois Field Basics

Galois fields will play an important role in the construction of Hadamard matrices. Thus we take a closer look here at some Galois field basics including a recipe to construct such fields . For the proofs of results stated in this part of the paper we refer to Herstein (1996) .

Let F be a field and let n be any positive integer . For $x \in F$ we define $n\,x = x + x + x + \ldots + x$ (n terms in the sum) . A field F is said to have *characteristic* m , if there exists a *smallest* positive number m such that $m\,x = 0$ for all $x \in F$. If no such positive integer m exists then F is said to have *characteristic zero* .

Let Z be the set of integers , and $n \geq 2$ be a fixed integer . For any $a , b \in Z$, we define $a \equiv b \,(\mathrm{mod}\, n)$ if and only if n divides $(a - b)$. One may check that $\equiv$ is an equivalence relation on Z . For $a \in Z$, we let $[u]$ be the equivalence class determined by u mod n . Then

$[u] = \{\, t\,n + a \;: t \in Z \,\}$ is called the *residue class* mod n determined by u .

Let Z_n be the quotient set of Z under $\equiv$. Then one can verify that $Z_n = \{\, [0] , [1] , [2] , \ldots , [n-1] \,\}$ (i.e. Z_n consists of n residue classes) .

In the set Z_n we introduce two operations, $+_n$ called *addition* mod n and $*_n$ called *multiplication* mod n as follows :

For $[a] , [b] \in Z_n$ define $[a] +_n [b] = [a + b]$ and $[a] *_n [b] = [a\,b]$. Then we can verify that $(Z_n , +_n , *_n)$ is a commutative ring with n

elements, called the *ring of integers* mod n. In general Z_n is not a field. To simplify the notation we will denote the element $[c]$ of Z_n by c.

Lemma 3.1 : Let F be a field. Then either F has characteristic zero (F is an infinite set and F contains an isomorphic copy of the rationals) or the characteristic of F is a prime number p (F may be a finite or infinite set and contains an isomorphic copy of the ring Z_p).

Lemma 3.2 : Z_n is a field if and only if n is a prime number.

Let Z_n be the ring of integers mod n. An expression of the form

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_k x^k$$

in an indeterminate x with $a_i \in Z_n$ is called a *polynomial* over Z_n. The elements a_i are called the *coefficients* of the polynomial. Further when $a_k \neq 0$, k is called the *degree* of $f(x)$, and when $a_k = [1]$, the unit element of Z_n, $f(x)$ is called *a monic* polynomial.

Let $Z_n[x] = \{ f(x) : f(x)$ polynomial over $Z_n \}$ be the set of all polynomials over Z_n. Let $f(x)$, $g(x)$ be polynomials in $Z_n[x]$. The *sum* of f and g, denoted by $f(x) + g(x)$, is obtained by adding coefficients of like powers of x. The *product* of f and g, denoted by $f(x)\,g(x)$, is obtained by term by term multiplication using the distributive law of Z_n, and then gathering together terms of like powers of x. Under these operations $Z_n[x]$ is a commutative ring with unit, called the *ring of polynomials* over Z_n. We will be interested in the ring $Z_p[x]$, where p is a prime number so that Z_p is a field. In all that follows p will denote a prime number.

Theorem 3.1 : [Factor Theorem]

Let $f(x)$, $g(x) \neq 0$ in $Z_p[x]$, and $c \in Z_p$ be given. Then

i) there exist unique $q(x)$ and $r(x)$ in $Z_p[x]$ such that $f(x) = g(x)\,q(x) + r(x)$, where $r(x) = 0$ or the degree of $r(x)$ is less than the degree of $g(x)$. The polynomial $r(x)$ is called the *remainder* and $q(x)$ is called the *quotient* ,

ii) the remainder in (i) dividing $f(x)$ in $Z_p[x]$ by $x - c$ is $f(c)$.

Let $f(x)$, $g(x) \neq 0$ in $Z_p[x]$ be given . We say $g(x)$ divides $f(x)$ ($g(x) \mid f(x)$) if and only if $f(x) = g(x)\, q(x)$ for some $q(x)$ in $Z_p[x]$. Then $g(x)$ is called a *factor* of $f(x)$.

Theorem 3.2 : [Remainder Theorem]
If $f(x) \in Z_p[x]$ and $c \in Z_p$, then $x - c$ in $Z_p[x]$ is a factor of $f(x)$ if and only if $f(c) = 0$.

A *Galois field* F is a field F in which the set F has a finite number of elements . We will denote a Galois field with s elements by writing $GF(s)$. By Lemma 3.2 , Z_p is a Galois field ($GF(p)$) , where p is any prime number , consisting of p elements. Let $f(x) \in Z_p[x]$ be given . Then any $c \neq 0$ in Z_p divides $f(x)$ since $f(x) = c\,(c^{-1} f(x))$. Hence any polynomial of the form $c\, f(x)$, $c \neq 0$ in Z_p will be called an *associate* of $f(x)$.

A polynomial $f(x) \in Z_p[x]$ is called *irreducible* over Z_p if and only if the only divisors of $f(x)$ are $f(x)$ and its associates . Those polynomials in $Z_p[x]$ which are irreducible over Z_p will play a key role in the construction of Galois fields . We now record some properties of Galois fields .

Theorem 3.3 : Let $F = GF(s)$ be a Galois field with s elements and let $F^* = F - \{0\}$. Then

i) $s = p^n$ for some number $n \geq 1$, and some prime p . This prime p is the characteristic of F .

ii) F^* under the multiplication of F is a cyclic group . Hence there exists some $a \in F^*$ such that $F^* = \{\, a^0 = 1,\ a^1,\ a^2,\ \ldots,\ a^{s-2} \,\}$. Such an "$a$" which generates F^* is called *a primitive element* of F^* .

iii) Let $q(x) \in Z_p[x]$ be an irreducible polynomial over Z_p , where p is a prime number and the characteristic of F . Then $q(x)$ divides $x^{s-1} - 1$.

iv) $x^s - x$ is a product of all the monic irreducible polynomials over $Z_p[x]$ of degree dividing n , where p is the prime characteristic of F

and $s = p^n$.

v) There exists a Galois field with p^n elements for any prime p.

Theorem 3.4 : Let $F = \{ 0, a_1, a_2, \ldots, a_{s-1} \}$ be a $GF(s)$, $s = p^n$, where p is a prime number . Then the polynomial $x^s - x$ in $Z_p[x]$ factorizes into linear factors

$$x^s - x = x(x - a_1)(x - a_2)\ldots(x - a_{s-1}).$$

Let F be a Galois field with $s = p^n$ elements . Then an irreducible polynomial $f(x) \in Z_p[x]$ is called a *primitive irreducible polynomial* if and only if $f(x)$ divides $x^m - 1$ for $m = p^n - 1 = s - 1$ but for no smaller m.

Now we give a recipe to construct a Galois field of order s, where $s = p^n$, p is a prime number , and $n \geq 1$ is an integer .

When $n = 1$, by Lemma 3.2 the ring Z_p is a $GF(p)$ under addition and multiplication mod p,

When $n \geq 2$, we consider the polynomial $x^s - x$ in $Z_p[x]$, and

i) Factorize $x^s - x$ into irreducible factors over $Z_p[x]$. Select all the irreducible polynomials in this factorization whose degree equals n. Let us say there are k of them $g_1(x), g_2(x), \ldots, g_k(x)$.

ii) From the $g_i's$ in (i) select those $g_i(x)$ which are primitive . We can develop the Galois field using any of these irreducible polynomials $g_i(x)$. However picking a primitive $g_i(x)$ gives a better description of the field for computational purposes . It actually provides a primitive element (a cyclic generator) for the field . From now on we will work with primitive irreducible polynomials .

iii) Suppose we have chosen a primitive irreducible polynomial of degree n from (ii). Let us call this selection $g(x)$. If we cannot decide on a primitive one , we can simply pick any $g_i(x)$ from (ii) .

iv) Let $F = \{ f(x) \in Z_p[x] : \text{degree of } f(x) \leq n - 1 \}$, i.e. F is the set of polynomials of the form $a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1}$ with $a_i \in Z_p$. Let $f_1(x)$, $f_2(x)$ be in F. To add $f_1(x)$ and $f_2(x)$, we do term by term addition of polynomials reducing the coefficients mod p. To multiply $f_1(x)$

with $f_2(x)$ we do the usual multiplication reducing the coefficients mod p. Then we divide this product by $g(x)$, where $g(x)$ is chosen in (iii) , and take the remainder as the product of f_1 with f_2 . We call this procedure of adding and multiplying mod$(p, g(x))$ *arithmetic* .

v) The set F defined under mod$(p, g(x))$ arithmetic is a Galois field of order p^n . To verify this , we refer to Herstein (1996) .

Consider a Galois field $GF(s)$ of order s, where $s = p^n$, with p an odd prime . An element $a \in GF(s)$ is called a *quadratic residue* (for short QR) if and only if there exists some $b \in GF(s)$ such that $a = b^2$. If no such b exists `$a$` is called a *quadratic nonresidue*. Note that 0 , 1 are always quadratic residues of $GF(s)$.

Let x be a primitive element of the multiplicative group $F^* = F - \{0\}$, where F is a $GF(s)$, $s = p^n$, p is an odd prime . Then all the quadratic residues of F are in the set $QR = \{ x^0, x^2, x^4, \ldots, x^{s-3} \}$.

We illustrate the steps (i) - (v) by developing some examples of Galois fields which will be useful later in this paper .

Example 3.1 : We construct $F = GF(7)$. Since 7 is a prime number we take $F = Z_7 = \{ 0, 1, 2, 3, 4, 5, 6 \}$ under mod 7 addition and multiplication . The addition and multiplication tables are given below :

$+_7$	0 1 2 3 4 5 6
0	0 1 2 3 4 5 6
1	1 2 3 4 5 6 0
2	2 3 4 5 6 0 1
3	3 4 5 6 0 1 2
4	4 5 6 0 1 2 3
5	5 6 0 1 2 3 4
6	6 0 1 2 3 4 5

$*_7$	0 1 2 3 4 5 6
0	0 0 0 0 0 0 0
1	0 1 2 3 4 5 6
2	0 2 4 6 1 3 5
3	0 3 6 2 5 1 4
4	0 4 1 5 2 6 3
5	0 5 3 1 6 4 2
6	0 6 5 4 3 2 1

Note that 3 is a primitive element of F and
$QR = \{ 0, 3^0, 3^2, 3^4 \} = \{ 0, 1, 2, 4 \}$.

Example 3.2 : We construct $GF(9)$. Note that $9 = 3^2$, so the base prime is 3 and the basic Galois field we work with is Z_3. Factorize $x^9 - x$ into irreducible polynomials over $Z_3[x]$:

$x^9 - x = x(x^8 - 1) = x(x^4 - 1)(x^4 + 1) = x(x - 1)(x + 1)(x^2 + 1)(x^2 + 2x + 2)(x^2 + x + 2)$

By Theorem 3.2.2 , the remainder theorem , the polynomials $g_1(x) = x^2 + 1$, $g_2(x) = x^2 + 2x + 2$, and $g_3(x) = x^2 + x + 2$ are irreducible. Of these the polynomial $g_1(x)$ is not primitive since $x^2 + 1 \mid x^4 - 1$. From the factorization of $x^9 - x$ it is clear the polynomials $g_2(x)$ and $g_3(x)$ are both primitive irreducible polynomials . We will work with $g_2(x)$.

Consider the set $F = \{ a_0 + a_1 x : a_0, a_1 \in Z_3[x] \}$, under $\bmod(3, g_2(x))$ arithmetic . Then F has the nine elements as follows :

$$\left.\begin{array}{ll} a_0 = 0, & a_1 = 0 \\ & a_1 = 1 \\ & a_1 = 2 \end{array}\right\} : \begin{array}{l} 0 \\ x, \\ 2x \end{array} \qquad \left.\begin{array}{ll} a_0 = 1, & a_1 = 0 \\ & a_1 = 1 \\ & a_1 = 2 \end{array}\right\} : \begin{array}{l} 1 \\ 1+x, \\ 1+2x \end{array}$$

$$\left.\begin{array}{ll} a_0 = 2, & a_1 = 0 \\ & a_1 = 1 \\ & a_1 = 2 \end{array}\right\} : \begin{array}{l} 2 \\ 2+x \\ 2+2x \end{array}$$

By Theorem 3.3 (ii) ,

$F^* = F - \{0\} = \{ 1, x, 1+x, 2x, 1+2x, 2, 2+x, 2+2x \}$ is a cyclic group under multiplication , and x is a primitive element (generator) for F^*. To verify this we calculate sucessive powers of x, using $\bmod(3, g_2(x))$ arithmetic to get:

0, $x^0 = 1$, $x^1 = x$, $x^2 = x + 1$ (replacing x^2 by $x + 1$),

$x^3 = x^2 + x = x + 1 + x = 2x + 1$,

$x^4 = x(2x + 1) = 2x^2 + x = 2x + 2 + x = 2$,

$x^5 = 2x$, $x^6 = 2x^2 = 2(x + 1) = 2x + 2$,

$x^7 = 2x^2 + 2x = 2x + 2 + 2x = x + 2$,

$x^8 = x^2 + 2x = x + 1 + 2x = 1$. Thus the powers of x generate F^*, and x is a primitive element of F^*.

Let us summarize our construction . The elements of F are

$F = \quad 0, 1, x, x^2, x^3, x^4, x^5, x^6, x^7 \qquad 0, 1, x, x \quad 1, 2x \quad 1, 2, 2x, 2x \quad 2, x \quad 2$

The mod $(3, g_2(x))$ arithmetic tables , one for addition and the other for multiplication are as follows :

$+_3$	0	1	x	x+1	2x+1	2	2x	2x+2	x+2
0	0	1	x	x+1	2x+1	2	2x	2x+2	x+2
1	1	2	x+1	x+2	2x+2	0	2x+1	2x	x
x	x	x+1	2x	2x+1	1	x+2	0	2	2x+2
x+1	x+1	x+2	2x+1	2x+2	2	x	1	0	2x
2x+1	2x+1	2x+2	1	2	x+2	2x	x+1	x	0
2	2	0	x+2	x	2x	1	2x+2	2x+1	x+1
2x	2x	2x+1	0	1	x+1	2x+2	x	x+2	2
2x+2	2x+2	2x	2	0	x	2x+1	x+2	x+1	1
x+2	x+2	x	2x+2	2x	0	x+1	2	1	2x+1

$+_3, *_3$	0	1	x	x+1	2x+1	2	2x	2x+2	x+2
0	0	0	0	0	0	0	0	0	0
1	0	1	x	x+1	2x+1	2	2x	2x+2	x+2
x	0	x	x+1	2x+1	2	2x	2x+2	x+2	1
x+1	0	x+1	2x+1	2	2x	2x+2	x+2	1	x
2x+1	0	2x+1	2	2x	2x+2	x+2	1	x	x+1
2	0	2	2x	2x+2	x+2	1	x	x+1	2x+1
2x	0	2x	2x+2	x+2	1	x	x+1	2x+1	2
2x+2	0	2x+2	x+2	1	x	x+1	2x+1	2	2x
x+2	0	x+2	1	x	x+1	2x+1	2	2x	2x+2

From the above presentation the quadratic residue set in $GF(9)$ is

$QR = \{ \ 0, \ x^0, \ x^2, \ x^4, \ x^6 \ \} = \{ \ 0, 1, x+1, 2, 2x+2 \ \}$.

Example 3.3 : We construct $F = GF(11)$. Since 11 is a prime number we take $F = Z_{11} = \{ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 \}$ under mod 11 arithmetic . The mod 11 addition and multiplication tables are as follows:

$+_{11}$	0	1	2	3	4	5	6	7	8	9	10
0	0	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10	0
2	2	3	4	5	6	7	8	9	10	0	1
3	3	4	5	6	7	8	9	10	0	1	2
4	4	5	6	7	8	9	10	0	1	2	3
5	5	6	7	8	9	10	0	1	2	3	4
6	6	7	8	9	10	0	1	2	3	4	5
7	7	8	9	10	0	1	2	3	4	5	6
8	8	9	10	0	1	2	3	4	5	6	7
9	9	10	0	1	2	3	4	5	6	7	8
10	10	0	1	2	3	4	5	6	7	8	9

$*_{11}$	0	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10
2	0	2	4	6	8	10	1	3	5	7	9
3	0	3	6	9	1	4	7	10	2	5	8
4	0	4	8	1	5	9	2	6	10	3	7
5	0	5	10	4	9	3	8	2	7	1	6
6	0	6	1	7	2	8	3	9	4	10	5
7	0	7	3	10	6	2	9	5	1	8	4
8	0	8	5	2	10	7	4	1	9	6	3
9	0	9	7	5	3	1	10	8	6	4	2
10	0	10	9	8	7	6	5	4	3	2	1

Note that 2 is a primitive element in $GF(11)$. Thus

$$QR = \{ 0, 2^0, 2^2, 2^4, 2^6, 2^8 \} = \{ 0, 1, 3, 4, 5, 9 \}.$$

Example 3.4 : To construct $F = GF(19)$, since 19 is a prime number then we take

$F = Z_{19} = \{ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18 \}$ under mod 19 arithmetic . The addition and multiplication tables may be constructed on the same principles as in Example 3.2.3 . Note that 3 is a primitive element mod 19 and the set of quadratic residues in F is $QR = \{ 1, 4, 5, 6, 7, 9, 11, 16, 17 \}$.

Example 3.5 : Suppose that the problem is to determine the quadratic residues and quadratic nonresidues in the Galois field $GF(25)$.

i) First we determine a quadratic primitive irreducible polynomial over Z_5. To this end we take the factor $x^{12}+1$ in the factorization $x^{24}-1 = (x^{12}-1)(x^{12}+1)$, and factorize it into irreducible factors over Z_5 (remember that the arithmetic on the coefficients is done mod 5) :

$$x^{12}+1 = (x^4)^3 + 1^3 = (x^4+1)(x^8 - x^4 + 1) .$$

Now

$$x^4+1=(x^2+2)(x^2+3),$$

$$x^8-x^4+1=(x^4+4)^2-(2x^2)^2=(x^4-2x^2+4)(x^4+2x^2+4)$$

$$x^4-2x^2+4=(x^2+2)^2-x^2=(x^2+x+2)(x^2-x+2)$$

$$x^4+2x^2+4=(x^2+3)^2-(2x)^2=(x^2+2x+3)(x^2-2x+3)$$

Thus

$$x^{12}+1=(x^2+2)(x^2+3)(x^2+x+2)(x^2-x+2)(x^2+2x+3)(x^2-2x+3)\ .$$

ii) Now $x^4+1=(x^2+2)(x^2+3)$ divides x^8-1 . Hence neither $g_1(x)=x^2+2$ nor $g_2(x)=x^2+3$ are primitive irreducible polynomials over Z_5. However, each of $g_3(x)=x^2+x+2$, $g_4(x)=x^2-x+2$, $g_5(x)=x^2+2x+3$ or $g_6(x)=x^2-2x+3$ are primitive irreducible polynomials over Z_5. Any of these may be used to develop $GF(25)$ giving both a multiplicative and additive representation to the elements of $GF(25)$. If either $g_1(x)$ or $g_2(x)$ is used we would obtain the additive representations of the elements of $GF(25)$ under mod$(5,\ g_i(x))$ arithmetic, $i=1,\ 2$, but not the multiplicative representation .

iii) Suppose we select $g(x)=g_3(x)=x^2+x+2$ to develop $GF(25)$. Then under mod$(5,\ x^2+x+2)$ arithmetic the set

$$F=\{x^i\ ;\ 0\le i\le 23\}\cup\{0\}$$

$$=\{\ ax+b\ :\ \ a\ ,\ b\in Z_5\ \}$$

is a Galois field of order 25 . Below we tabulate the elements of F in their multiplicative and additive form :

0	1	x	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9	x^{10}
0	1	x	$4x+3$	$4x+2$	$3x+2$	$4x+4$	2	$2x$	$3x+1$	$3x+4$	$x+4$

x^{11}	x^{12}	x^{13}	x^{14}	x^{15}	x^{16}	x^{17}	x^{18}	x^{19}	x^{20}	x^{21}	x^{22}	x^{23}
$3x+3$	4	$4x+4$	$x+2$	$x+3$	$2x+3$	$x+1$	3	$3x+2$	4	$2x+1$	$4x+1$	$2x+2$

iv) From the table in (iii): the quadratic residues in $GF(25)$ is the set

$QR=\{\ 0\ ,\ 1\ ,\ 4x+3\ ,\ 3x+2\ ,\ 2\ ,\ 3x+1\ ,\ x+4\ ,\ 4\ ,\ x+2\ ,\ 2x+3\ ,\ 3\ ,\ 2x+4\ ,\ 4x+1\ \}$.

The quadratic nonresidues in $GF(25)$ is the set

$\{\ x\ ,\ 4x+2\ ,\ 4x+4\ ,\ 2x\ ,\ 3x+4\ ,\ 3x+3\ ,\ 4x\ ,\ x+3\ ,\ x+1\ ,\ 3x\ ,\ 2x+1\ ,\ 2x+2\ \}$.

Remarks :

a) It is interesting to note that in Example 3.5, 2 and 3 are quadratic nonresidues in $Z_5 = GF(5)$ but are quadratic residues in $GF(25)$.

b) One can establish that there are exactly $\frac{(p^2 - p)}{2}$ monic irreducible quadratic polynomials over Z_p , p a prime . For the case $p = 5$, there are thus $\frac{(25 - 5)}{2} = 10$ monic irreducible quadratic polynomials over Z_5. Six of these are given in (ii) of Example 3.5 . The remaining four of these monic irreducible quadratic polynomials appear as factors of $x^{12} - 1$:

$$x^{12} - 1 = (x^6 - 1)(x^6 + 1)$$

$$= (x - 1)(x + 1)(x + 2)(x + 3)(x^2 + x + 1)(x^2 - x + 1)(x^2 + 2x + 4)(x^2 - 2x + 4) .$$

Of course none of these four monic irreducible quadratic polynomials are primitive since each divides $x^{12} - 1$.

4. Paley's Constructions

Firstly, we have shown that for the even prime $p = 2$ and any positive integer k a Hadamard matrix of order $n = 2^k$ may be constructed by repeatedly taking the Kronecker product of $H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ with itself k times . This raises the question of the construction of Hadamard matrices whose order n is related to an odd prime power. In this connection Paley (1933) offered the following two constructions :

(P1) a Hadamard matrix of order $n = s + 1$ can be constructed where s is a prime power , say $s = p^r$, p a prime and $s \equiv 3 \pmod 4$.

(P2) a Hadamard matrix of order $n = 2(s + 1)$ can be constructed, where $s = p^r$ is a power of a prime p and $s \equiv 1 \pmod 4$.

The purpose of this part is to develop and present the Paley constructions outlined in (P1) and (P2) . Both involve the use of Galois fields $GF(s)$. Unlike the Kronecker product construction which requires at least one pre-existing Hadamard matrix to implement it , the Paley

construction produces a Hadamard matrix once the order of the matrix is specified as in (P1) or (P2) .

The following notation and setting will be used in the formulation of the results below. Let $F = GF(s)$ be a Galois field of order s where $s = p^r$ and p is an odd prime number. Let $H = \{1,-1\}$ be the two element multiplicative subgroup of the multiplicative group of the nonzero real numbers . Recall that the set of nonzero elements of F , call it F^*, is a cyclic group under multiplication . The following mapping χ, known as a *character* , and some of its properties will be helpful in detailing the Paley constructions : $\chi : F^* \to H$ is the mapping defined by

$$\chi(a) = \begin{cases} 1, & a \text{ is a quadratic residue in } F^* , \\ -1, & a \text{ is a quadratic nonresidue in } F^* . \end{cases}$$

Lemma 4.1 : The character $\chi : F^* \to H$ is a group homomorphism between the two multiplicative groups .

Proof : Note that the product of two nonzero quadratic residues or the product of two quadratic nonresidues is a quadratic residue , whereas the product of a nonzero quadratic residue and a quadratic nonresidue is a quadratic nonresidue . From this it is immediate that $\chi(a\,b) = \chi(a)\,\chi(b)$ for all a , b in F^* and the lemma is established. □

Corollary 4.1 : In F there are precisely $\frac{s+1}{2}$ quadratic residues and $\frac{s-1}{2}$ quadratic nonresidues . Moreover $\sum_{a \in F^*} \chi(a) = 0$.

Proof : From Lemma 4.1 , the kernel of χ consists of the quadratic residues in F^* and the only other coset of χ consists of the quadratic nonresidues . Since the cardinality of F^* , $|F^*| = s-1$, it follows that F^* has $\frac{s-1}{2}$ quadratic residues and $\frac{s-1}{2}$ quadratic nonresidues . Since the zero element 0 in F is also a quadratic residue the total number of quadratic residues in F is $\frac{s+1}{2}$ and the corollary is established . □

Lemma 4.2 :

i) When $s = p^r \equiv 1 \pmod 4$ then -1 is a quadratic residue in F.

ii) When $s = p^r \equiv 3 \pmod 4$ then -1 is a quadratic nonresidue in F.

Proof : Let x be a primitive element (generator) of the cyclic group F^*. Since the order of F^* is $s-1$ we conclude that $x^{s-1} = 1$. Hence $(x^{(s-1)/2} - 1)(x^{(s-1)/2} + 1) = 0$. Since F is a field and the order of x is $s-1$ we conclude that $x^{(s-1)/2} + 1 = 0$ or $x^{(s-1)/2} = -1$. When $s \equiv 1 \pmod 4$ then $s = 4k+1$ for some integer k. Then $x^{(s-1)/2} = x^{2k} = (x^k)^2 = -1$ and -1 is a quadratic residue establishing (i) . When $s \equiv 3 \pmod 4$ then $s = 4m+3$ for some integer m. Then $x^{(s-1)/2} = x^{2m+1} = -1$ and x is a quadratic nonresidue establishing (ii) . □

Corollary 4.2 :

i) When $s = p^r \equiv 1 \pmod 4$ then $\chi(-a) = \chi(a)$ for all a in F^*.

ii) When $s = p^r \equiv 3 \pmod 4$ then $\chi(-a) = -\chi(a)$ for all a in F^*.

Proof : Using Lemma 4.1 , for any $a \in F$ we have $\chi(-a) = \chi((-1)(a)) = \chi(-1)\chi(a)$. When $s \equiv 1 \pmod 4$, $\chi(-1) = 1$ and when $s \equiv 3 \pmod 4$, $\chi(-1) = -1$ by Lemma 4.2 and the definition of χ. From this both (i) and (ii) follow completing the proof . □

In the following it will be useful to extend the definition of the character χ to all of F by placing $\chi(0) = 0$, where the first 0 is the zero element of F and the second zero is the real number 0 . With this extended definition we have χ as a map from F to the set $\{-1,0,1\}$. The following lemma will be most helpful in establishing our first main result .

Lemma 4.3 : $\sum_{b \in F} \chi(b)\chi(b+c) = -1$, if $c \neq 0$.

Proof : $\chi(0)\ \chi(0+c) = 0$ .Since F is a field , when $b \neq 0$, b^{-1} exists . Let $z = b^{-1}(b+c)$. Then $z \neq 0$ when $b \neq -c$, and z is the *unique* element in F such that $bz = b + c$. Let $K = \{\, z = b^{-1}(b+c) \ : b \in F^*, b \neq -c \,\}$. We note that $K = F^* - \{1\}$, where 1 is the unit element of F. Note that $b^{-1}(b+c) \neq 1$ for any $b \in F^*$, for otherwise $b + c = b$ from which $c = 0$, a contradiction .

Hence $K \subseteq F^* - \{1\}$. Next , let $x \in F^* - \{1\}$. Define $b = c(x-1)^{-1}$. Then $b \neq 0$, for otherwise $c = 0$ or $x = 1$, neither of which is the case . Moreover $b^{-1}(b+c) = c^{-1}(x-1)[c(x-1)^{-1} + c] = 1 + (x-1) = x$ from which we conclude that $x \in K$. Hence $F^* - \{1\} \subseteq K$. In all $K = F^* - \{1\}$. Now ,

$\sum_{b \in F} \chi(b)\chi(b+c) = \sum_{b \in F^*} \chi(b)\chi(b+c) = \sum_{z \in F^* - \{1\}} \chi(b)\chi(bz)$, since

$K = F^* - \{1\}$. By Lemma 4.1, $\chi(bz) = \chi(b)\chi(z)$ and thus

$\sum_{b \in F} \chi(b)\chi(b+c) = \sum_{z \in F^* - \{1\}} [\chi(b)]^2 \chi(z) = \sum_{z IN F^* - \{1\}} \chi(z) = \sum_{z \in F^*} \chi(z) - \chi(1) = 0 - 1 = -1$,

using Corollary 4.1 . □

A real matrix M of order n is called *skew symmetric* if and only if $M = -M'$. It is clear that any skew symmetric matrix has each of its diagonal entries equal to zero. Recall that a Hadamard matrix H of order n is called a *skew Hadamard* matrix if and only if $H = I_n + S$, where S is a skew symmetric matrix . Clearly to obtain a skew Hadamard matrix we need a skew symmetric matrix whose off diagonal entries are +1 or -1.

We now introduce a matrix Q of order $s = p^r$, p an odd prime , and study its properties in the lemmas below . This matrix Q will play a crucial role in both Paley constructions. The definition of Q is based on the Galois field F of order $s = p^r$, p an odd prime and uses the character χ defined on F : let $F = \{ \alpha_- , \alpha_1 , \alpha_2 , \ldots , \alpha_{s-1} \}$ be a listing of the s elements of F with $\alpha_- = 0$. Define

$$Q = (q_{ij})_{sxs} \quad , \quad q_{ij} = \chi(\alpha_j - \alpha_i) \qquad (3.1)$$

Lemma 4.4 : The matrix Q is a matrix with entries in the set $\{-1,0,1\}$. When $s = p^r \equiv 1 \pmod 4$ then Q is a symmetric matrix . When $s = p^r \equiv 3 \pmod 4$ then Q is a skew symmetric matrix .

Proof : The first statement of the lemma follows from the definition of the character χ .

Moreover

$$q_{ij} = \chi(\alpha_j - \alpha_i) = \chi((-1)(\alpha_i - \alpha_j)) = \begin{cases} -\chi(\alpha_i - \alpha_j), \text{when } p^r \equiv 3 \pmod 4, \\ \chi(\alpha_i - \alpha_j), \text{when } p^r \equiv 1 \pmod 4, \end{cases}$$

$$= \begin{cases} -q_{ji}, \text{when } p^r \equiv 3 \pmod 4, \\ q_{ji}, \text{when } p^r \equiv 1 \pmod 4, \end{cases}$$

using Corollary 4.2 . This completes the proof . □

The following notation will be useful and will be employed throughout : J_{mxn} will denote a matrix of order mxn each of whose entries is +1 . We simply write J when its dimension is apparent from the context.

Lemma 4.5 : Q satisfies the following :

i) $QQ' = s\,I_s - J$,

ii) $Q\,J = J\,Q = 0$,

Proof :

i) Let $Q'Q = B = (b_{ij})$, then

b_{ij} = inner product of the i-th row of Q with the j-th row of Q

$= \sum_k q_{ik}\ q_{jk} = \sum_k \chi(\alpha_k - \alpha_i)\,\chi(\alpha_k - \alpha_j) = s - 1$ if $i = j$, and equals -1 if $i \neq j$ using Lemma 4.3 and taking $b = \alpha_k - \alpha_i$ and $c = \alpha_i - \alpha_j \neq 0$ in that lemma . This establishes (i).

ii) $QJ = 0$ follows from $\sum_j \chi(\alpha_i - \alpha_j) = 0$ using Corollary 4.1 . □

We now use the matrix Q defined in (3.1) , to define the following matrix which is of major importance in the Paley constructions :

$$S = \begin{pmatrix} 0 & -J_{1xs} \\ J_{sx1} & Q \end{pmatrix}_{(s+1)x(s+1)} \qquad (3.2)$$

Lemma 4.6 : Let $s = p^r$, p an odd prime , with $p \equiv 3 \pmod 4$. Then the matrix S defined in (3.2) has the properties :

i) $S' = -S$, namely S is skew symmetric ,

ii) $S'S = s\,I_{s+1}$.

Proof :

i) This follows from Lemma 4.4 , since Q is skew symmetric when $p \equiv 3 \pmod 4$.

ii) $$SS' = \begin{pmatrix} 0 & -J_{1\times s} \\ J_{s\times 1} & Q \end{pmatrix}\begin{pmatrix} 0 & J_{1\times s} \\ -J_{s\times 1} & Q' \end{pmatrix} = \begin{pmatrix} s & \underline{0}' \\ \underline{0} & QQ' + J_{s\times s} \end{pmatrix} = sI_{s+1},$$

using Lemma 4.5 (i). This completes the proof . □

We are now ready to give the first Paley construction (the construction outlined in statement (P1)) .

Theorem 4.1 : [The First Paley construction ; Paley (1933)]

Let $s = p^r$, p an odd prime , with $p \equiv 3 \pmod 4$. Then the matrix $H_{s+1} = I_{s+1} + S$, where S is defined as in (3.2) is a skew Hadamard matrix of order $s+1$.

Proof :

$H'H = (I+S)(I+S') = I + S + S' + S\,S' = I + S - S + s\,I_{s+1} = (s+1)\,I_{s+1}$, using Lemma 4.6 . Hence H is a skew Hadamard matrix of order $s+1$. This completes the proof . □

We illustrate Theorem 4.1 by constructing a Hadamard matrix of order 28 . This presented in the following example .

Example 4.1 : To make the presentation self contained we recall some definitions from the second part of this paper . In addition we will require the Remainder Theorem [Theorem 3.2] and two other theorems quoted below ; the proofs of the latter two theorems may be found in any standard book on abstract algebra which discusses Galois fields, for example, Herstein (1996) .

Throughout p will denote a prime, $n \geq 1$ will be an integer and let $s = p^n$.

A polynomial $f(x)$ in the polynomial ring $Z_p[x]$ will be called *reducible* iff $f(x) = g_1(x)\,.\,g_2(x)$ for some $g_i \in Z_p[x]$ with degree g_i < degree f for $i = 1, 2$ .Otherwise f is called *irreducible.* Moreover, $f(x)$ is called *monic* iff the coefficient of its highest degree term is 1 . An irreducible polynomial

$f(x)$ in $Z_p[x]$ is called *primitive* iff $f(x)$ divides the polynomial $x^m - 1$ for $m = s - 1$ but does not divide $x^m - 1$ for any m such that $1 \le m < s - 1$.

The importance of irreducible polynomials stems from the following :

(GF1) let $g(x)$ in $Z_p[x]$ be any monic irreducible polynomial of degree n ,

(GF2) let $F = \{ \quad f(x) \quad : \quad f(x) \in Z_p[x] \quad , \text{degree } f(x) \le n - 1 \quad \}$.

Then the underlying set F under mod$(\ p\ ,\ g(x))$ arithmetic is a Galois field of order s . We write $GF(s)$ as a shorthand for the Galois field of order s and it denotes the pair $(\ F\ ,\ \text{mod}(\ p\ ,\ g(x)))$ where $g(x)$ is defined in (GF1) and F in (GF2).

Let $F^* = F - \{0\}$. We have mentioned in the second part that F^* is a cyclic group under the multiplication in F . The importance of monic irreducible primitive polynomials is due to the following :

(GF4) if the monic irreducible polynomial $g(x)$ in (GF1) is also primitive then the cyclic group F^* is generated by the polynomial $q(x) = x$ in F under mod$(\ p\ ,\ g(x))$ arithmetic . In fact F^* has $\phi(s - 1)$ generators, where ϕ is the Euler ϕ - function, and $F^* = \{ \quad x^i \quad : \quad 0 \le i \le s - 2 \quad \}$. Thus $x^t \in F^*$ is also a generator of F^* iff

$t \le s - 1$ and t is relatively prime to $s - 1$.

The above discussion raises two questions :

Question 1 : How does one find monic irreducible polynomials $g(x)$ in $Z_p[x]$ of degree n ?

Question 2 : How does one find monic irreducible primitive polynomials in $Z_p[x]$ of degree n ?

Let us consider the special polynomial $Q_s(x) = x^s - x$. An answer to both questions can be given in terms of factorizing $Q_s(x)$ in $Z_p[x]$. The answer is not too satisfactory, as we shall see, because often $Q_s(x)$ is very difficult to factorize .

Theorem A : (i) Let $g(x)$ be any monic irreducible polynomial of degree dividing n . Then $g(x)$ divides $Q_s(x)$.

(ii) The polynomial $Q_s(x)$ equals the product of all monic irreducible polynomials whose degrees divide n .

(iii) The number of monic irreducible polynomials of degree n is equal to $\frac{[\phi(s-1)]}{n}$ where ϕ is the Euler ϕ-function .

The next result reduces the labour involved in checking that an irreducible polynomial of degree n is primitive in certain cases .

Theorem B : Suppose that $p \equiv 3 \pmod 4$. Let $g(x)$ be a monic irreducible polynomial of degree n . Consider the Galois field $GF(s) = (F, \text{mod}(p, g(x))$. Then,

if $x^{(s-1)/2} = -1$ under $\text{mod}(p, g(x))$ arithmetic then $g(x)$ is primitive .

We are now ready to construct H_{28} using the first Paley method . We give the construction procedure in steps . In this construction we need to develop $GF(3^3)$ so that $n = p = 3$ and $s = 27$.

Step 1. Find a cubic monic primitive irreducible polynomial in $Z_3[x]$. At first glance this step seems easy . According to Theorem A we need to factorize $Q_3(x) = x^{27} - x$ into irreducibles of degree dividing 3 . The polynomial we seek is among the factors . Now $x^{27} - x = x(x^{13} - 1)(x^{13} + 1)$ and by the Remainder Theorem $x^{13} - 1$ and $x^{13} + 1$ have $x - 1$ and $x + 1$ as factors respectively . Upon division by $x - 1$ and $x + 1$ we are left with two lengthy 12 degree polynomials which are indeed very difficult to factorize . So we abandon this approach and try a different strategy .

This strategy works well when n is small and prime . We now present the strategy as a sequence of problems and solutions .

A cubic monic polynomial in $Z_3[x]$ has the form : $a + b\,x + c\,x^2 + x^3$ with a , b , c in Z_3 . Hence there are precisely 27 such polynomials .

Problem 1 . Find all the cubic monic reducible polynomials in $Z_3[x]$.

Solution . Using the Remainder Theorem it may be verified that the list of 19 monic cubic polynomials are all reducible :

(i) $x^3 - x;\quad x^3 + x;\quad x^3 + x^2;\quad x^3 - x^2;\quad x^3 - x^2 - x;\quad x^3 + x^2 - x;\quad x^3 - x^2 + x;\quad x^3 + x^2 + x;\quad x^3$,

(ii) $x^3 - 1;\quad x^3 + x^2 + 1;\quad x^3 + x + 1;\quad x^3 - x^2 - x + 1;\quad x^3 - x^2 + x - 1;\quad x^3 + x^2 - x - 1$,

(iii) $x^3 + 1;\quad x^3 - x^2 - 1;\quad x^3 + x^2 + x + 1;\quad x^3 + x - 1$.

In fact $q(x)$ is in (i) iff $q(0) = 0$; $q(x)$ is in (ii) iff $q(1) = 0$ and $q(x)$ is in (iii) iff $q(2) = 0$.

Problem 2 . Find all the cubic monic irreducible polynomials in $Z_3[x]$.

Solution. The purpose of Problem 1 was to eliminate the 19 Monic reducible polynomials of the possible 27 monic cubic polynomials . The remaining 8 must be monic irreducible and hence any of them is suitable to develop $GF(3^3)$. We list the 8 in 2 groups :

(PI) $x^3 - x - 2;\quad x^3 - x^2 - 2;\quad x^3 + x^2 - x + 1;\quad x^3 - x^2 + x + 1$,

(NPI) $x^3 - x^2 - x - 1;\quad x^3 - x - 1;\quad x^3 + x^2 + x - 1;\quad x^3 + x^2 - 1$.

Again the Remainder Theorem may be used to verify that the 8 polynomials listed in (PI) and (NPI) are irreducible .

Problem 3. [This problem addresses Step 1] . Find a monic cubic primitive irreducible polynomial in $Z_3[x]$.

Solution. The polynomial we seek is among the 8 polynomials listed in the solution to Problem 2 . By Theorem A (iii) there are $\frac{\phi(26)}{3} = \frac{12}{3} = 4$ such cubic primitive irreducibles .

There is no quick method of identifying which 4 amongst the 8 are primitive . We resort to a well known mathematical technique : trial and error . We simply pick one of the 8 listed polynomials and apply Theorem B to it and continue on until we are succesful . In this way we find that the 4 polynomials listed in the group (PI) are primitive and the remaining 4 are not. As an illustration let us verify that the irreducible polynomial $g(x) = x^3 - x - 2$ is primitive. Consider $GF(3^3)$ under mod $(3\ ,\ g(x))$ arithmetic . Then under this arithmetic we have the *reduction relation*

(RR) : $x^3 = x + 2$

Now under mod $(3\ ,\ g(x))$ arithmetic we have

$$\begin{aligned} x^{12} = (x^3)^4 &= (x+2)^4 \text{ using (RR)} \\ &= x^4 + 2x^3 + 2x + 1 \quad \text{, expanding} \\ &= x(x+2) + 2(x+2) + 2x + 1 \text{ using (RR)} \\ &= x^2 + 2 \end{aligned}$$

Hence $x^{13} = x(x^2 + 2) = x^3 + 2x = x + 2 + 2x$ using (RR) .

$= 2 = -1$,

That is, $x^{13} = -1$ and by Theorem B, $g(x)$ is primitive .

The next problem is now unnecessary but it illustrates Theorem A .

Problem 4. Factorize $Q_s(x) = x^{27} - x$ to illustrate Theorem A .

Solution. In this case $n = 3$. Thus the only irreducibles of degree

Dividing $n = 3$ are of degree 1 or 3 . Those of degree 1 are Clearly x , $x-1$, $x+1$ and those of degree 3 are listed in (PI) and (NPI) . Hence

$$x^{26}-1 = \left[\begin{array}{l} (x+1)\,(x^3-x-2)\,(x^3-x^2-2)\,(x^3+x^2-x+1)\,(x^3-x^2+x+1) \\ \\ (x-1)\,(x^3-x^2-x-1)\,(x^3-x-1)\,(x^3+x^2+x-1)\,(x^3+x^2-1) \end{array} \right]$$

Indeed the factors in the first line multiply out to $x^{13}+1$ and those in the second line multiply out to $x^{13}-1$

Step 2. Select a monic cubic primitive irreducible polynomial and use it to develop $GF(3^3)$. Write the elements of F in both the additive form and as powers of its cyclic generator x .

This is the second crucial step in the construction process . We choose the cubic primitive irreducible polynomial $g(x) = x^3 - x - 2$. The underlying set F of $GF(3^3)$ is then $F = \{\ a x^2 + b x + c \ : \ a\ ,\ b\ ,\ c \in Z_3 \ \}$, and F under mod $(3\ ,\ g(x) = x^3 - x - 2)$ arithmetic is a Galois field of order 27. To facilitate computation under mod$(3\ ,\ g(x))$ arithmetic we will, as before, use the reduction relation :

$$\text{(RR)} : \quad x^3 = x + 2 \ .$$

Since $g(x)$ is primitive the cyclic group $F^* = F - \{0\}$ has x as a generator . Hence $F^* = \{\ x^i \ : \ 0 \le i \le 25 \ \}$. For convenience, we rename the 27 elements of F as follows:

$\alpha_{-1} = 0$ (zero element of F) , $\alpha_{\_} = x^{\infty} = 1$ (unit element of F) , and in general $\alpha_i = x^i$, $0 \le i \le 25$. Before we develop the additive (polynomial) and power form for each element of F , a very crucial step for the Paley construction, let us demonstrate a particular calculation by finding the additive form of $x^5 \in F^*$. We use (RR) as often as necessary. Now $x^5 = x^2(x^3) = x^2(x+2) = x^3 + 2x^2 = x + 2 + 2x^2 = 2x^2 + x + 2$. Thus the additive form of x^5 is $2x^2 + x + 2$. Using this method we can develop the additive form of each x^i . Since $g(x)$ is primitive, we are guaranteed that we can do 26 such calculations in succession and thereby exhaust F^* obtaining the additive form of each element of F . In the table below we record the 27 elements of F in their additive and power forms and identify each with the appropriate symbol α_i .

Elements of F in the additive and power form		
$\alpha_{-1}=0$	$\alpha_8=x^8=2x^2+2$	$\alpha_{17}=x^{17}=2x^2+x$
$\alpha_0=x^0=1$	$\alpha_9=x^9=x+1$	$\alpha_{18}=x^{18}=x^2+2x+1$
$\alpha_1=x$	$\alpha_{10}=x^{10}=x^2+x$	$\alpha_{19}=x^{19}=2x^2+2x+2$
$\alpha_2=x^2$	$\alpha_{11}=x^{11}=x^2+x+2$	$\alpha_{20}=x^{20}=2x^2+x+1$
$\alpha_3=x^3=x+2$	$\alpha_{12}=x^{12}=x^2+2$	$\alpha_{21}=x^{21}=x^2+1$
$\alpha_4=x^4=x^2+2x$	$\alpha_{13}=x^{13}=2$	$\alpha_{22}=x^{22}=2x+2$
$\alpha_5=x^5=2x^2+x+2$	$\alpha_{14}=x^{14}=2x$	$\alpha_{23}=x^{23}=2x^2+2x$
$\alpha_6=x^6=x^2+x+1$	$\alpha_{15}=x^{15}=2x^2$	$\alpha_{24}=x^{24}=2x^2+2x+1$
$\alpha_7=x^7=x^2+2x+2$	$\alpha_{16}=x^{16}=2x+1$	$\alpha_{25}=x^{25}=2x^2+1$

(T)

Step 3. Construct the Paley matrix $Q=(q_{ij})$ of order 27 defined in (3.1) of part three .

Recall that the entries q_{ij} are defined as follows :

$$q_{ij}=\begin{cases}0 \quad , \ if \ \ i=j \\ 1 \quad , \ if \ \ i\neq j \ \ and \ \ \alpha_j-\alpha_i \ \ is \ \ a \ quadratic \ residue \ in \ F \ , \\ -1 \quad , \ if \ \ i\neq j \ \ and \ \ \alpha_j-\alpha_i \ \ is \ \ a \ quadratic \ nonresidue \ in \ F \ .\end{cases}$$

The Paley matrix Q will be presented in partitioned form $Q=[\ Q_1|Q_2\ ]$, where Q_1 is of order *27x15* and Q_2 is of order *27x12* at the end of this example . The vertical and horizontal margins will be labelled by the elements α_i of F . Crucial to developing the entries of Q is table (T) of Step 2 . We illustrate how table (T) helps in developing Q by solving the next problem .

Problem 5. (i) Compute the entries $q_{4,22}$ and $q_{4,8}$ of Q.

(ii) Explain why $q_{ij}=-q_{ji}$ for all i , j .

Solution .

(i) Now $\alpha_{22}-\alpha_5=x^{22}-x^5=(2x+2)-(2x^2+x+2)=x^2+x=x^{10}$, using table

(T) twice . Since x^{10} is a quadratic residue in F , $q_{5,22} = 1$.

Similarly, $\alpha_8 - \alpha_4 = x^8 - x^4 = (2x^2 + 2) - (x^2 + 2x) = x^2 - 2x + 2 = x^{11}$, using table (T) twice . Since x^{11} is a quadratic nonresidue in F , $q_{4,8} = -1$.

(ii) Now $\alpha_j - \alpha_i = -(\alpha_i - \alpha_j)$. Also $x^{13} = -1$ from table (T) . Suppose that $\alpha_j - \alpha_i = x^k$. Then $\alpha_i - \alpha_j = -(\alpha_j - \alpha_i) = x^{13} . x^k = x^{k+13}$. Thus $k + 13$ is even iff k is odd and $k + 13$ is odd iff k is even . Hence $q_{ij} = -q_{ji}$.

Step 4 . We are now ready to construct H_{28} the Hadamard matrix of order 28 .

First we form the matrix S of order 28 defined in (3.2) of part three :

$$S = \begin{pmatrix} 0 & -J_{1x27} \\ J_{27x1} & Q \end{pmatrix},$$

where Q is the Paley matrix developed in Step 3 and J_{27x1} is a vector each of whose entries is +1 . Finally set

$$H_{28} = I_{28} + S,$$

where I_{28} is the identity matrix of order 28 . Due to Theorem 3.3.1, we know that H_{28} is a Hadamard matrix of order 28 . From Problem 5 (ii), we know that Q is skew symmetric and hence so is S . Thus by definition, the matrix H_{28} constructed here is a skew Hadamard matrix . It is interesting to note that each diagonal entry of H_{28} is +1 .

$Q_1 =$

	α_{-1}	α_0	α_1	α_2	α_3	α_4	α_5	α_6	α_7	α_8	α_9	α_{10}	α_{11}	α_{12}	α_{13}
α_{-1}	0	+	−	+	−	+	−	+	−	+	−	+	−	+	−
α_0	-	0	-	+	-	-	+	+	+	-	-	-	+	-	+
α_1	+	+	0	+	-	+	+	-	-	-	+	+	+	-	+
α_2	-	-	-	0	-	+	-	-	+	+	+	-	-	-	+
α_3	+	+	+	+	0	+	-	+	+	-	-	-	+	+	+
α_4	-	+	-	-	-	0	-	+	-	-	+	+	+	-	-
α_5	+	-	-	+	+	+	0	+	-	+	+	-	-	-	+
α_6	-	-	+	+	-	-	-	0	-	+	-	-	+	+	+
α_7	+	-	+	-	-	+	+	+	0	+	-	+	+	-	-
α_8	-	+	+	-	+	+	-	-	-	0	-	+	-	-	+
α_9	+	+	-	-	+	-	-	+	+	+	0	+	-	+	+
α_{10}	-	+	-	+	+	-	+	+	-	-	-	+	-	+	-
α_{11}	+	-	-	+	-	-	+	-	-	+	+	+	0	+	-
α_{12}	-	+	+	+	-	+	+	-	+	+	-	-	-	0	-
α_{13}	+	-	-	-	-	+	-	-	+	-	-	+	+	+	0
α_{14}	-	-	+	+	+	+	-	+	+	-	+	+	-	-	-
α_{15}	+	-	+	-	-	-	-	+	-	-	+	-	-	+	+
α_{16}	-	-	+	-	+	+	+	+	-	+	+	-	+	+	-
α_{17}	+	+	+	-	+	-	-	-	-	+	-	-	+	-	-
α_{18}	-	-	-	-	+	-	+	+	+	+	-	+	+	-	+
α_{19}	+	-	+	+	+	-	+	-	-	-	-	+	-	-	+
α_{20}	-	+	+	-	-	-	+	-	+	+	+	+	-	+	+
α_{21}	+	-	-	-	+	+	+	-	+	-	-	-	-	+	-
α_{22}	-	-	+	+	+	-	-	-	+	-	+	+	+	+	-
α_{23}	+	+	+	-	-	-	+	+	+	-	+	-	-	-	-
α_{24}	-	+	-	-	+	+	+	-	-	-	+	-	+	+	+
α_{25}	+	+	-	+	+	-	-	-	+	+	+	-	+	-	-

$Q_2 =$

	α_{14}	α_{15}	α_{16}	α_{17}	α_{18}	α_{19}	α_{20}	α_{21}	α_{22}	α_{23}	α_{24}	α_{25}
α_{-1}	+	-	+	-	+	-	+	-	+	-	+	-
α_0	+	+	+	-	+	+	-	+	+	-	-	-
α_1	-	-	-	-	+	-	-	+	-	-	+	+
α_2	-	+	+	+	+	-	+	+	-	+	+	-
α_3	-	+	-	-	-	-	+	-	-	+	-	-
α_4	-	+	-	+	+	+	+	-	+	+	-	+
α_5	+	+	-	+	-	-	-	-	+	-	-	+
α_6	-	-	-	+	-	+	+	+	+	-	+	+
α_7	-	+	+	+	-	+	-	-	-	-	+	-
α_8	+	+	-	-	-	+	-	+	+	+	+	-
α_9	-	-	-	+	+	+	-	+	-	-	-	-
α_{10}	-	+	+	+	-	-	-	+	-	+	+	+
α_{11}	+	+	-	-	-	+	+	+	-	+	-	-
α_{12}	+	-	-	+	+	+	-	-	-	+	-	+
α_{13}	+	-	+	+	-	-	-	+	+	+	-	+
α_{14}	0	-	+	-	-	+	+	+	-	-	-	+
α_{15}	+	0	+	-	+	+	-	-	-	+	+	+
α_{16}	-	-	0	-	+	-	-	+	+	+	-	-
α_{17}	+	+	+	0	+	-	+	+	-	-	-	+
α_{18}	+	-	-	-	0	-	+	-	-	+	+	+
α_{19}	-	-	+	+	+	0	+	-	+	+	-	-
α_{20}	-	+	+	-	-	-	0	-	+	-	-	+
α_{21}	-	+	-	-	+	+	+	0	+	-	+	+
α_{22}	+	+	-	+	+	-	-	-	0	-	+	-
α_{23}	+	-	-	+	-	-	+	+	+	0	+	-
α_{24}	+	-	+	+	-	+	+	-	-	-	0	-
α_{25}	-	-	+	-	-	+	-	-	+	+	+	0

We now develop the second Paley construction (outlined in statement (P2)) . This construction is based on the concept of a conference matrix . A *conference matrix* , hereafter called a *C-matrix* , is a matrix M of order n such that the diagonal entries of M are zero , the off-diagonal entries are +1 or -1 and $M'M = (n - 1) I_n$. Clearly , if M is a C-matrix then $M'M = (n - 1) I_n$ so that every pair of rows (or columns) of M are orthogonal . C-matrices were first used by Belevitch (1950) in studying the theoretical aspects of electrical networks . Later they were studied in their own right by Goethals and Seidel (1967) who in fact referred to these matrices as conference matrices . Since the second Paley construction depends on the existence of

C-matrices we state two results below without proof which shed some light on the question of their existence.

Let m be a positive integer and suppose $m = n^2 (p_1\ p_2\ p_3 \ldots\ p_k)$ where $p_i (1 \le i \le k)$ are distinct prime numbers . Then the number $t = p_1\ p_2\ p_3 \ldots\ p_k$ is called the *square free* part of m. The following two - square theorem is a well known number theoretic result and includes the celebrated two square Fermat theorem as a special case . We refer for the proof to Hardy and Wright (1954) .

Theorem 4.2 : [Two Square Theorem]

A positive integer $m = x^2 + y^2$, for some integers x and y if and only if the square free part of m consists of prime numbers each of which is congruent to $1 (\mod 4)$. The connection of the two square theorem to C-matrices occurs via the next theorem. For a proof of this next theorem see Raghavarao (1971) and Wallis et al (1972) .

Theorem 4.3 : A necessary condition for the existence of a square rational matrix M (i.e. M has rational number entries) of order $n \equiv 2 (\mod 4)$ satisfying $M'M = m I_n$ for some positive integer m is that $m = a^2 + b^2$ for some integers a and b.

A clear inference from Theorem 4.2 and 4.3 is the following :

Corollary 4.3 : A necessary condition that there exist a C-matrix of order $n \equiv 2 (\mod 4)$ is that the square free part of $n - 1$ consists of prime numbers each of which is congruent to $1 (\mod 4)$.

From Corollary 4.3 we conclude that there are many values of $n \equiv 2 (\mod 4)$ for which a C-matrix of order n does not exist . For examples C-matrices of orders $n = 22, 34, 58, 78, \ldots, etc$ .do not exist . For a listing of orders <1000 for which C-matrices exist and those orders excluded by the above results see Wallis et al (1972).

For certain $n \equiv 2 (\mod 4)$ a C-matrix of this order n always exist . Indeed the developments earlier in this part guarantees this . To ferret out this pleasant situation we adjust the definition of S given in (3.2) .

Consider the matrix T of order $s+1$ defined as follows :

$$T = T_{s+1} = \begin{pmatrix} 0 & J_{1xs} \\ J_{sx1} & Q \end{pmatrix}_{(s+1)x(s+1)} \qquad (3.3)$$

where the matrix Q is defined in (3.1) .

Lemma 4.7 : Suppose that the order $s = p^r$, p an odd prime , of the Galois field F satisfies $s \equiv 1 \pmod 4$. Let T be the matrix of order $s+1$ defined in (3.3). Then T is a symmetric C-matrix .

Proof : Since $s \equiv 1 \pmod 4$, Q is symmetric by Lemma 4.4 and hence so is T . Further , as in the proof of Lemma 4.6 ,

$T'T = \begin{pmatrix} s & \underline{0'} \\ \underline{0} & QQ' + J_{sxs} \end{pmatrix} = s\, I_{s+1}$, using Lemma 4.5 (i) . Hence T is a C-matrix , completing the proof . □

We remark that the matrix S of order $s+1$ defined in (3.2) is also a C-matrix but it is not symmetric . The second Paley construction requires a symmetric C-matrix and this necessitates the adjustment of S to T as done in (3.3) .

Example 4.2 : We construct the symmetric C-matrix T_6. First $GF(5) = \{0, 1, 2, 3, 4\}$ under $+_5$, $*_5$. The quadratic residues of $GF(5)$ is the set $QR = \{0, 1, 4\}$ and the quadratic nonresidues is the set $\{2, 3\}$. Thus

$$Q = \begin{pmatrix} 0 & + & - & - & + \\ + & 0 & + & - & - \\ - & + & 0 & + & - \\ - & - & + & 0 & + \\ + & - & - & + & 0 \end{pmatrix}_{5x5} \quad \text{and} \quad T_6 = \begin{pmatrix} 0 & + & + & + & + & + \\ + & 0 & + & - & - & + \\ + & + & 0 & + & - & - \\ + & - & + & 0 & + & - \\ + & - & - & + & 0 & + \\ + & + & - & - & + & 0 \end{pmatrix}_{6x6} .$$

It may be verified that $T_6\ T_{6'} = T_{6'}\ T_6 = 5\, I_6$.

Example 4.3 : We construct the symmetric C-matrix T_{10}. First, as in Example 3.2, we consider
$GF(9)=\{\ 0,\ x^{-}=1,\ x^{1}=x,\ x^{2}=x+1,\ x^{3}=2x+1,\ x^{4}=2,\ x^{5}=2x,\ x^{6}=2x+2,\ x^{7}=x+2\ \}$ under mod $(3,\ x^{2}+2x+2)$ arithmetic . The set of quadratic residues of $GF(9)$ is $QR=\{\ 0,\ 1,\ x+1,\ 2,\ 2x+2\ \}$ and the set of quadratic nonresidues is $\{\ x,\ 2x+1,\ 2x,\ x+2\ \}$. Thus the matrix $Q=(q_{ij})$ of order 9 defined in (3.1) is displayed below (the horizontal and vertical margins are indexed by the elements of $GF(9)$) :

$Q =$

	0	1	x	x+1	2 x+1	2	2 x	2 x+2	x+2
0	0	1	-1	1	-1	1	-1	1	-1
1	1	0	-1	-1	-1	1	1	-1	1
x	-1	-1	0	1	1	1	-1	-1	1
x+1	1	-1	1	0	-1	-1	-1	1	1
2 x+1	-1	-1	1	-1	0	1	1	1	-1
2	1	1	1	-1	1	0	-1	-1	-1
2 x	-1	1	-1	-1	1	-1	0	1	1
2 x+2	1	-1	-1	1	1	-1	1	0	-1
x+2	-1	1	1	1	-1	-1	1	-1	0

Then the symmetric C-matrix T_{10} defined in (3.3) is obtained from Q by bordering it as follows :

$$T_{10} = \begin{pmatrix} 0 & 1' \\ 1 & Q \end{pmatrix}_{10x10} .$$

Theorem 4.4 : [Second Paley Construction ; Paley (1933)]

i) If a symmetric C-matrix M of order n exists then the matrix

$$H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes M + \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} \otimes I_n \qquad (3.4)$$

where $\otimes$ is the Kronecker product , is a symmetric Hadamard matrix of order $2n$.

ii) If T is the symmetric C-matrix of order $s+1$ defined in (3.3) ,where $s = p^{r} \equiv 1 \pmod 4$ and p is an odd prime , then

$$H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes T + \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} \otimes I_n$$

is a symmetric Hadamard matrix of order $2s+2$.

Proof : (ii) is immediate from (i) and Lemma 4.7 . Hence we prove (i) . Note that H defined in (3.4) can be rewriten as

$$H = \begin{pmatrix} M+I & M-I \\ M-I & -(M+I) \end{pmatrix}.$$ Now by direct multiplication ,

$$HH' = \begin{pmatrix} M+I & M-I \\ M-I & -(M+I) \end{pmatrix} \begin{pmatrix} M'+I & M'-I \\ M'-I & -(M'+I) \end{pmatrix} = 2nI,$$

performing the block multiplication and using $M = M'$ and $M'M = (n-1)I_n$.

□

The Paley constructions given in Theorems 4.1 and 4.4 form the backbone of a number of further construction results on Hadamard matrices based on Galois fields which have been developed since Paley's initial effort in 1933 described here . At this point we simply summarize some of these additional construction results below . We emphasize that these are actual constructions when the stated conditions are met , as are the Paley theorems , and not merely existence statements . For detailed proofs of these results see Hall (1967) . As in first part , the constructions below are of the recursive type , and use the Kronecker product when appropriate .

Theorem 4.5 : [Williamson (1944) ; Generalization of Paley's second Construction]
If $s = p^r \equiv 1 \pmod 4$, p a prime and if a Hadamard matrix H of order $n > 1$ is given then a Hadamard matrix of order $n(s+1)$ can be constructed .

Theorem 4.6 :

i) Let $n = 2^t k_1 k_2 \dots k_m$. Suppose that either $k_i = p_i^{r_i} + 1 \equiv 0 \pmod 4$ or $k_i = 2(p_i^{r_i} + 1)$, $p_i^{r_i} \equiv 1 \pmod 4$ for each i . Then a symmetric Hadamard matrix of order n can be constructed .

ii) Let a skew Hadamard matrix of order n be given . Suppose that $s = p^r \equiv 3 \pmod 4$, where p is a prime . Then a skew Hadamard matrix of order $n(s+1)$ can be constructed .

iii) Let $n = 2^t k_1 k_2 \dots k_m$ where each $k_i = p_i^{r_i} + 1 \equiv 0 \pmod 4$ with p_i

prime . Then a skew Hadamard matrix of order n can be constructed .

iv) Let a skew Hadamard matrix of order n be given . Then a Hadamard matrix of order $n(n-1)$ can be constructed .

v) Let a skew Hadamard matrix of order n and a symmetric Hadamard matrix of order $m = n+4$ be given. Then a Hadamard matrix of order $n(n+3)$ can be constructed.

vi) Let two Hadamard matrices of orders $n_1 > 1$ and $n_2 > 1$ be given . Let p be a prime such that $p^r \equiv 1 \pmod 4$. Then a Hadamard matrix of order $n_1 n_2 (p^r + 1) p^r$ can be constructed .

vii) Let two Hadamard matrices of orders $n_1 > 1$ and $n_2 > 1$ be given . Suppose that n is a positive number such that $n = p_1^{r_1} + 1$ for some prime p_1 and $n+4 = p_2^{r_2} + 1$ for some prime p_2. Then a Hadamard matrix of order $n_1 n_2 n(n+3)$ can be constructed .

We now give some examples to illustrate the two Paley constructions .

Example 4.4 : To construct a Hadamard matrix of order 8 , we observe that 8=7+1 . The quadratic residues of $GF(7) = \{0,1,2,3,4,5,6\}$ is the set $QR = \{0,1,2,4\}$ and the quadratic nonresidues is the set $\{3,5,6\}$. Using (3.1) , and (3.2) we construct the matrix Q and the matrix S

$$Q = \begin{pmatrix} 0 & - & - & + & - & + & + \\ + & 0 & - & - & + & - & + \\ + & + & 0 & - & - & + & - \\ - & + & + & 0 & - & - & + \\ + & - & + & + & 0 & - & - \\ - & + & - & + & + & 0 & - \\ - & - & + & - & + & + & 0 \end{pmatrix}_{7x7}, \quad S = \begin{pmatrix} 0 & -J_{1x7} \\ J_{7x1} & Q_{7x7} \end{pmatrix}_{8x8}.$$

Finally , by Theorem 4.1 , $H_8 = I_8 + S$:

$$H_8 = \begin{pmatrix} + & - & - & - & - & - & - & - \\ + & + & - & - & + & - & + & + \\ + & + & + & - & - & + & - & + \\ + & + & + & + & - & - & + & - \\ + & - & + & + & + & - & - & + \\ + & + & - & + & + & + & - & - \\ + & - & + & - & + & + & + & - \\ + & - & - & + & - & + & + & + \end{pmatrix}_{8x8} .$$

Example 4.5 : To construct a Hadamard matrix H_{12} of order 12 , there are two ways . First we observe that 12=11+1 . The quadratic residues of $GF(11)=\{\ 0,1,2,3,4,5,6,7,8,9,10\ \}$ is the set $QR=\{\ 0,1,3,4,5,9\ \}$ and the quadratic nonresidues is the set $\{\ 2,6,7,8,10\ \}$. Using (3.1) , and (3.2) , the matrices Q and S are

$$Q = \begin{pmatrix} 0 & - & + & - & - & - & + & + & + & - & + \\ + & 0 & - & + & - & - & - & + & + & + & - \\ - & + & 0 & - & + & - & - & - & + & + & + \\ + & - & + & 0 & - & + & - & - & - & + & + \\ + & + & - & + & 0 & - & + & - & - & - & + \\ + & + & + & - & + & 0 & - & + & - & - & - \\ - & + & + & + & - & + & 0 & - & + & - & - \\ - & - & + & + & + & - & + & 0 & - & + & - \\ - & - & - & + & + & + & - & + & 0 & - & + \\ + & - & - & - & + & + & + & - & + & 0 & - \\ - & + & - & - & - & + & + & + & - & + & 0 \end{pmatrix}_{11x11} ,$$

$$S = \begin{pmatrix} 0 & -J_{1x11} \\ J_{11x1} & Q_{11x11} \end{pmatrix}_{12x12} .$$

Thus , by Theorem 4.1 , $H_{12} = I_{12} + S$ is the skew Hadamard matrix displayed below:

$$H_{12} = \begin{pmatrix} + & - & - & - & - & - & - & - & - & - & - & - \\ + & + & - & + & - & - & - & + & + & + & - & + \\ + & + & + & - & + & - & - & - & + & + & + & - \\ + & - & + & + & - & + & - & - & - & + & + & + \\ + & + & - & + & + & - & + & - & - & - & + & + \\ + & + & + & - & + & + & - & + & - & - & - & + \\ + & + & + & + & - & + & + & - & + & - & - & - \\ + & - & + & + & + & - & + & + & - & + & - & - \\ + & - & - & + & + & + & - & + & + & - & + & - \\ + & - & - & - & + & + & + & - & + & + & - & + \\ + & + & - & - & - & + & + & + & - & + & + & - \\ + & - & + & - & - & - & + & + & + & - & + & + \end{pmatrix}_{12x12} .$$

Now we construct H_{12} by the second Paley construction . As 12=2(5+1) , where 5 is a prime and $5 + 1 \equiv 2 \pmod 4$, we can use Theorem 4.4 and Example 4.2 to construct H_{12}. From Example 4.2, and Theorem 4.4 (ii) ,

$$T_6 = \begin{pmatrix} 0 & + & + & + & + & + \\ + & 0 & + & - & - & + \\ + & + & 0 & + & - & - \\ + & - & + & 0 & + & - \\ + & - & - & + & 0 & + \\ + & + & - & - & + & 0 \end{pmatrix}_{6x6} , \text{ and } H_{12} = \begin{pmatrix} T_6 + I_6 & T_6 - I_6 \\ T_6 - I_6 & -(T_6 + I_6) \end{pmatrix} .$$

Hence H_{12} is the symmetric Hadamard matrix displayed below :

$$H_{12} = \begin{pmatrix} + & + & + & + & + & + & - & + & + & + & + & + \\ + & + & + & - & - & + & + & - & + & - & - & + \\ + & + & + & + & - & - & + & + & - & + & - & - \\ + & - & + & + & + & - & + & - & + & - & + & - \\ + & - & - & + & + & + & + & - & - & + & - & + \\ + & + & - & - & + & + & + & + & - & - & + & - \\ - & + & + & + & + & + & - & - & - & - & - & - \\ + & - & + & - & - & + & - & - & - & + & + & - \\ + & + & - & + & - & - & - & - & - & - & + & + \\ + & - & + & - & + & - & - & + & - & - & - & + \\ + & - & - & + & - & + & - & + & + & - & - & - \\ + & + & - & - & + & - & - & - & + & + & - & - \end{pmatrix}_{12x12}.$$

Example 4.6 : We construct a Hadamard matrix of order 20 by the Second Paley construction . As 20=2(9+1), where 9 is a power of a prime and $9+1 \equiv 2 \pmod 4$, we can use Theorem 4.4 and Example 4.3 to construct H_{20} as follows (we display T_{10} below, it is obtained from Example 4.3) :

$$T_{10} = \begin{pmatrix} 0 & + & + & + & + & + & + & + & + & + \\ + & 0 & + & - & + & - & + & - & + & - \\ + & + & 0 & - & - & - & + & + & - & + \\ + & - & - & 0 & + & + & + & - & + & - \\ + & + & - & + & 0 & - & - & - & + & + \\ + & - & - & + & - & 0 & + & + & + & - \\ + & + & + & + & - & + & 0 & - & - & - \\ + & - & + & - & - & + & - & 0 & + & + \\ + & + & - & - & + & + & - & + & 0 & - \\ + & - & + & + & + & - & - & + & - & 0 \end{pmatrix}_{10\times 10},$$

and then by Theorem 4.4 (ii)

$$H_{20} = \begin{pmatrix} T_{10}+I_{10} & T_{10}-I_{10} \\ T_{10}-I_{10} & -(T_{10}+I_{10}) \end{pmatrix}.$$

A full display of H_{20} is below :

$H_{20} =$

$$\begin{pmatrix}
+ & + & + & + & + & + & + & + & + & + & - & + & + & + & + & + & + & + & + & + \\
+ & + & + & - & + & - & + & - & + & - & + & - & + & - & + & - & + & - & + & - \\
+ & + & + & - & - & - & + & + & - & + & + & + & - & - & - & - & + & + & - & + \\
+ & - & - & + & + & + & + & - & - & + & + & - & - & - & + & + & + & - & - & + \\
+ & + & - & + & + & - & - & - & + & + & + & + & - & + & - & - & - & - & + & + \\
+ & - & - & + & - & + & + & + & + & - & + & - & - & + & - & - & + & + & + & - \\
+ & + & + & + & - & + & + & - & - & - & + & + & + & + & - & + & - & - & - & - \\
+ & - & + & - & - & + & - & + & + & + & + & - & + & - & - & + & - & - & + & + \\
+ & + & - & - & + & + & - & + & + & - & + & + & - & - & + & + & - & + & - & - \\
+ & - & + & + & + & - & - & + & - & + & + & - & + & + & + & - & - & + & - & - \\
- & + & + & + & + & + & + & + & + & + & - & - & - & - & - & - & - & - & - & - \\
+ & - & + & - & + & - & + & - & + & - & - & - & - & + & - & + & - & + & - & + \\
+ & + & - & - & - & - & + & + & - & + & - & - & - & + & + & + & - & - & + & - \\
+ & - & - & - & + & + & + & - & - & + & - & + & + & - & - & - & - & + & + & - \\
+ & + & - & + & - & - & - & - & + & + & - & - & + & - & - & + & + & + & - & - \\
+ & - & - & + & - & - & + & + & + & - & - & + & + & - & + & - & - & - & - & + \\
+ & + & + & + & - & + & - & - & - & - & - & - & - & - & + & - & - & + & + & + \\
+ & - & + & - & - & + & - & - & + & + & - & + & + & - & + & - & - & - & - & - \\
+ & + & - & - & + & + & - & + & - & - & - & + & + & - & - & + & - & - & + & \\
+ & - & + & + & + & - & - & + & - & - & - & + & - & - & - & + & + & - & + & - \\
\end{pmatrix}_{20\times 20}$$

References

[1]. Belevitch, V. 1950. Theory of 2^n - terminal networks with application to conference telephony. *Electron*. *Commun*. 27: 231-244 .

[2]. Goethals, J. M. and Seidel, J. J. 1967. Orthogonal matrices with zero diagonal. *Canad. J. Math*. 19: 1001-1010 .

[3]. Hardy, G. H., and Wright, E. M. 1954. *An introduction to the theory of numbers*. Oxford University Press, London .

[4]. Hall, M. 1967. *Combinatorial Theory*. Blaisdell (Ginn), Waltham, Mass .

[5]. Herstein, I. N. 1996. *Abstract Algebra,* third edition. Prentice-Hall Inc., New Jersey.

[6]. Leghwel A., "On Some Characterizations of Hadamard Matrices", Journal of Humanities and Applied Science, June issue no. 24 (2014), 20-41 .

[7]. Paley, R. E. A. C. 1933. On orthogonal matrices. *J. Math. and Physics*. 12: 311-320.

[8]. Ragahavarao, D. 1971. *Constructions and Combinatorial Problems in Design of Experiments*. John Wiley and Sons Inc., New York .

[9]. Wallis, W. D. and Street, Anne Penfold. 1972. *Combinatorics : Room squares, sum-free sets, Hadamard matrices*. Lecture Notes in Mathematics 292. Springer-Verlag, Berlin, Heidelberg, New York .

[10]. Williamson, J. 1944. Hadamard's determinant theorem and the sum of four squares. *Duke Math. J.* 11: 65-81 .

On Some Methods of Constructing Hadamard Matrices

Abdurzak M. Leghwel [1]

Abstract

There are two methods , often used to produce examples of algebraic and combinatorial structures . One of these methods begins with at least one example of the desired structure at hand and then constructs further structures of a like kind . We call such a construction method *recursive*. Another method (or methods) is to generate the desired structure simply after certain parameters regarding it have been specified . We shall call such a method of construction an *ab initio* method .

Hadamard matrices are algebraic structures in the sense that they form an important subclass of the class of matrices and hence must conform to all the algebraic rules obeyed by matrices under the usual operations of addition and multiplication . On the other hand , Hadamard matrices are combinatorial structures as well since the entries +1 and -1 of which the matrix consists must follow certain patterns . Thus one expects that one should be able to utilize both type of constructions methods , recursive and ab initio , to construct Hadamard matrices . This is indeed the case and in this paper we review some of these construction methods for Hadamard matrices .

In the second part we will introduce the concept of the Kronecker product and develop a recursive construction method for constructing Hadamard matrices based on it . Two important ab initio methods are discussed in the fourth part of this paper. These methods are due to Paley (1933) and is based on Galois fields . Hence some Galois field basics are presented in the third part also.

Keywords : Hadamard Matrix, Kronecker product, Galois fields.

1. Introduction

A (-1,1) - *matrix* is a matrix whose only entries are the numbers -1 or 1 . In this paper for the most part we will be interested in special (-1,1)-matrices called Hadamard matrices .

[1] Department of Mathematics, Faculty of Science, Alasmarya Islamic University, Zliten – Libya .

A *Hadamard matrix* of order n is an nxn (-1,1)- matrix H, satisfying $H'H = H'H = n I_n$, where H' denotes the transpose of H and I_n is the identity matrix of order n. If H is a Hadamard matrix, it follows from the definition that the set of row vectors of H, as well as, the set of column vectors of H form mutually orthogonal sets . The reader is referred to [6].

2. Construction of Hadamard Matrices Based on The Kronecker Product

In this part we present the construction of Hadamard matrices employing the Kronecker product . This construction is recursive and requires at least one Hadamard matrix at hand in order to utilize it . It is , therefore , most useful when employed in conjunction with some of the other techniques for constructing Hadamard matrices to be developed later . We begin by introducing the concept of the Kronecker product of matrices and some of its basic properties .

Definition : If $A = (a_{ij})$ is a pxq matrix and $B = (b_{ij})$ is a rxs matrix , then their *Kronecker product* $A \otimes B$ is the $prxqs$ matrix given by

Example 2.1 : If $A = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}_{2x2}$, $B = \begin{pmatrix} 2 & 4 \\ -5 & 3 \end{pmatrix}_{2x2}$,

then $$A \otimes B = \begin{pmatrix} 2 & 4 & 2 & 4 \\ -5 & 3 & -5 & 3 \\ 2 & 4 & -2 & -4 \\ -5 & 3 & 5 & -3 \end{pmatrix}_{4x4}$$

The basic properties concerning how the Kronecker product $\otimes$ relates to the matrix operations of addition , multiplication , scalar multiplication and transpose are given in the following theorem .

Theorem 2.1 : Let $A = (a_{ij})$ be a pxq matrix and $B = (b_{ij})$ be a rxs matrix. The Kronecker product $A \otimes B$ is a $prxqs$ matrix with the following properties :

i) $\alpha(A \otimes B) = (\alpha A) \otimes B = A \otimes (\alpha B)$ for any real number α ,

ii) $(A_1 + A_2) \otimes B = (A_1 \otimes B) + (A_2 \otimes B)$ and
$A \otimes (B_1 + B_2) = (A \otimes B_1) + (A \otimes B_2)$,

iii) $(A_1 \otimes B_1)(A_2 \otimes B_2) = A_1 A_2 \otimes B_1 B_2$, where the matrices A_i and B_i respectively are compatible for multiplication ,

iv) $(A \otimes B)' = A' \otimes B'$,

v) $(A \otimes B) \otimes C = A \otimes (B \otimes C)$ for any matrix C ,

vi) $(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}$, if A^{-1} and B^{-1} exist .

Proof : We will prove property (iv) , and we refer to a standard text in linear algebra for the rest .

Since

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1q}B \\ a_{21}B & a_{22}B & \cdots & a_{2q}B \\ \vdots & & & \\ a_{p1}B & a_{p2}B & \cdots & a_{pq}B \end{pmatrix}_{pr \times qs}, \quad (A \otimes B)' = \begin{pmatrix} a_{11}B' & a_{21}B' & \cdots & a_{p1}B' \\ a_{12}B' & a_{22}B' & \cdots & a_{p2}B' \\ \vdots & & & \\ a_{1q}B' & a_{2q}B' & \cdots & a_{pq}B' \end{pmatrix}_{qs \times pr} = A' \otimes B' .$$

□

The relationship between the determinant of the Kronecker product of square matrices and the determinant of individual matrices is given in the following :

Theorem 2.2 : For any two square matrices A of order m and B of order n, $\det(A \otimes B) = [\det(A)]^n [\det(B)]^m$.

Proof : We prove the theorem for the case when A has order $m = 2$.

Then $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}_{2x2}$ .If all $a_{ij} = 0$ then the theorem is clearly true . Hence , without loss of generality suppose that $a_{11} \neq 0$. Then

$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B \\ a_{21}B & a_{22}B \end{pmatrix}$. Further , we may also assume without loss of generality that $\det(B) \neq 0$. Then by [6, Theorem 3.1] ,

$\det(A \otimes B) = [\det(a_{11}B)]\,[\det(a_{22}B - a_{21}B(a_{11}B)^{-1}a_{12}B)]$

$= [\det(a_{11}B)][\det(a_{22}B - a_{21}a_{11}^{-1}a_{12}B)]$

$= \det[a_{11}B(a_{22}B - a_{21}a_{11}^{-1}a_{12}B)]$

$= \det[(a_{11}a_{22} - a_{21}a_{12})B^2] = (a_{11}a_{22} - a_{21}a_{12})^n \det(B^2)$

$= \det[A]^n \det[B^2] = [\det(A)]^n [\det(B)]^2$ and the theorem is proved for the case $m = 2$. □

From the viewpoint of Hadamard matrices , the properties of the Kronecker product immediately imply the following result :

Theorem 2.3 : If H_1 and H_2 are Hadamard matrices of orders n_1 and n_2 respectively , then $H_1 \otimes H_2$ is a Hadamard matrix of order $n_1 n_2$.

Proof : Let H_1 and H_2 be a Hadamard matrices of orders n_1 and n_2 respectively . Then

$(H_1 \otimes H_2)(H_1 \otimes H_2)' = (H_1 \otimes H_2)(H_{1'} \otimes H_{2'}) = H_1 H_{1'} \otimes H_2 H_{2'}$

$= n_1 I_{n_1} \otimes n_2 I_{n_2} = n_1 n_2 I_{n_1 n_2}$. □

Corollary 2.1. : Since there is a Hadamard matrix of order 2 , namely $H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, then there are Hadamard matrices of order 2^n for every positive integer n.

Proof : $H_{2^n} = H_2 \otimes H_2 \otimes \ldots \otimes H_2$, the Kronecker product of H_2 with itself extended over n factors gives the desired Hadamard matrix of order 2^n. □

Corollary 2.2 : If H is a Hadamard matrix of order k, for some positive integer k then there is a Hadamard matrix of order $2^n k$ for every positive integer n.

Proof : Let $H_1 = H \otimes H_{2^n}$, where H is a Hadamard matrix of order k, and H_{2^n} is the Hadamard matrix of order 2^n given in Corollary 2.1 . Then by Theorem 2.3, H_1 is a Hadamard matrix of order $2^n k$. □

Example 2.2 : Let H_2 be the normalized Hadamard matrix of order 2 . The matrix

$H_4 = H_2 \otimes H_2 = \begin{pmatrix} + & + & + & + \\ + & - & + & - \\ + & + & - & - \\ + & - & - & + \end{pmatrix}_{4x4}$ is a Hadamard matrix of order 4 .

By Theorem 2.3, we conclude that $H_{64} = H_4 \otimes H_4 \otimes H_4$ is a Hadamard matrix of order 64 .

Theorem 2.3 will be more helpful when we apply it to Hadamard matrices constructed by other methods . We discuss some of these other methods below .

3. Some Galois Field Basics

Galois fields will play an important role in the construction of Hadamard matrices. Thus we take a closer look here at some Galois field basics including a recipe to construct such fields . For the proofs of results stated in this part of the paper we refer to Herstein (1996) .

Let F be a field and let n be any positive integer . For $x \in F$ we define $n\,x = x + x + x + \ldots + x$ (n terms in the sum) . A field F is said to have *characteristic* m , if there exists a *smallest* positive number m such that $m\,x = 0$ for all $x \in F$. If no such positive integer m exists then F is said to have *characteristic zero* .

Let Z be the set of integers , and $n \geq 2$ be a fixed integer . For any $a , b \in Z$, we define $a \equiv b \,(\mathrm{mod}\, n)$ if and only if n divides $(a - b)$. One may check that $\equiv$ is an equivalence relation on Z . For $a \in Z$, we let $[u]$ be the equivalence class determined by u mod n . Then

$[u] = \{\, t\,n + a \;: t \in Z \,\}$ is called the *residue class* mod n determined by u .

Let Z_n be the quotient set of Z under $\equiv$. Then one can verify that $Z_n = \{\, [0] , [1] , [2] , \ldots , [n-1] \,\}$ (i.e. Z_n consists of n residue classes) .

In the set Z_n we introduce two operations, $+_n$ called *addition* mod n and $*_n$ called *multiplication* mod n as follows :

For $[a] , [b] \in Z_n$ define $[a] +_n [b] = [a + b]$ and $[a] *_n [b] = [a\,b]$. Then we can verify that $(Z_n , +_n , *_n)$ is a commutative ring with n

elements, called the *ring of integers* mod n. In general Z_n is not a field. To simplify the notation we will denote the element $[c]$ of Z_n by c.

Lemma 3.1 : Let F be a field. Then either F has characteristic zero (F is an infinite set and F contains an isomorphic copy of the rationals) or the characteristic of F is a prime number p (F may be a finite or infinite set and contains an isomorphic copy of the ring Z_p).

Lemma 3.2 : Z_n is a field if and only if n is a prime number.

Let Z_n be the ring of integers mod n. An expression of the form

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_k x^k$$

in an indeterminate x with $a_i \in Z_n$ is called a *polynomial* over Z_n. The elements a_i are called the *coefficients* of the polynomial. Further when $a_k \neq 0$, k is called the *degree* of $f(x)$, and when $a_k = [1]$, the unit element of Z_n, $f(x)$ is called *a monic* polynomial.

Let $Z_n[x] = \{ f(x) : f(x)$ polynomial over $Z_n \}$ be the set of all polynomials over Z_n. Let $f(x)$, $g(x)$ be polynomials in $Z_n[x]$. The *sum* of f and g, denoted by $f(x) + g(x)$, is obtained by adding coefficients of like powers of x. The *product* of f and g, denoted by $f(x)\,g(x)$, is obtained by term by term multiplication using the distributive law of Z_n, and then gathering together terms of like powers of x. Under these operations $Z_n[x]$ is a commutative ring with unit, called the *ring of polynomials* over Z_n. We will be interested in the ring $Z_p[x]$, where p is a prime number so that Z_p is a field. In all that follows p will denote a prime number.

Theorem 3.1 : [Factor Theorem]

Let $f(x)$, $g(x) \neq 0$ in $Z_p[x]$, and $c \in Z_p$ be given. Then

i) there exist unique $q(x)$ and $r(x)$ in $Z_p[x]$ such that $f(x) = g(x)\,q(x) + r(x)$, where $r(x) = 0$ or the degree of $r(x)$ is less than the degree of $g(x)$. The polynomial $r(x)$ is called the *remainder* and $q(x)$ is called the *quotient* ,

ii) the remainder in (i) dividing $f(x)$ in $Z_p[x]$ by $x - c$ is $f(c)$.

Let $f(x)$, $g(x) \neq 0$ in $Z_p[x]$ be given . We say $g(x)$ divides $f(x)$ ($g(x) \mid f(x)$) if and only if $f(x) = g(x)\, q(x)$ for some $q(x)$ in $Z_p[x]$. Then $g(x)$ is called a *factor* of $f(x)$.

Theorem 3.2 : [Remainder Theorem]
If $f(x) \in Z_p[x]$ and $c \in Z_p$, then $x - c$ in $Z_p[x]$ is a factor of $f(x)$ if and only if $f(c) = 0$.

A *Galois field* F is a field F in which the set F has a finite number of elements . We will denote a Galois field with s elements by writing $GF(s)$. By Lemma 3.2 , Z_p is a Galois field ($GF(p)$) , where p is any prime number , consisting of p elements. Let $f(x) \in Z_p[x]$ be given . Then any $c \neq 0$ in Z_p divides $f(x)$ since $f(x) = c\,(c^{-1} f(x))$. Hence any polynomial of the form $c\, f(x)$, $c \neq 0$ in Z_p will be called an *associate* of $f(x)$.

A polynomial $f(x) \in Z_p[x]$ is called *irreducible* over Z_p if and only if the only divisors of $f(x)$ are $f(x)$ and its associates . Those polynomials in $Z_p[x]$ which are irreducible over Z_p will play a key role in the construction of Galois fields . We now record some properties of Galois fields .

Theorem 3.3 : Let $F = GF(s)$ be a Galois field with s elements and let $F^* = F - \{0\}$. Then

i) $s = p^n$ for some number $n \geq 1$, and some prime p . This prime p is the characteristic of F .

ii) F^* under the multiplication of F is a cyclic group . Hence there exists some $a \in F^*$ such that $F^* = \{\, a^0 = 1,\ a^1,\ a^2,\ \ldots,\ a^{s-2} \,\}$. Such an "$a$" which generates F^* is called *a primitive element* of F^* .

iii) Let $q(x) \in Z_p[x]$ be an irreducible polynomial over Z_p , where p is a prime number and the characteristic of F . Then $q(x)$ divides $x^{s-1} - 1$.

iv) $x^s - x$ is a product of all the monic irreducible polynomials over $Z_p[x]$ of degree dividing n , where p is the prime characteristic of F

and $s = p^n$.

v) There exists a Galois field with p^n elements for any prime p.

Theorem 3.4 : Let $F = \{ 0, a_1, a_2, \ldots, a_{s-1} \}$ be a $GF(s)$, $s = p^n$, where p is a prime number . Then the polynomial $x^s - x$ in $Z_p[x]$ factorizes into linear factors

$$x^s - x = x(x - a_1)(x - a_2)\ldots(x - a_{s-1}).$$

Let F be a Galois field with $s = p^n$ elements . Then an irreducible polynomial $f(x) \in Z_p[x]$ is called a *primitive irreducible polynomial* if and only if $f(x)$ divides $x^m - 1$ for $m = p^n - 1 = s - 1$ but for no smaller m.

Now we give a recipe to construct a Galois field of order s, where $s = p^n$, p is a prime number , and $n \geq 1$ is an integer .

When $n = 1$, by Lemma 3.2 the ring Z_p is a $GF(p)$ under addition and multiplication mod p,

When $n \geq 2$, we consider the polynomial $x^s - x$ in $Z_p[x]$, and

i) Factorize $x^s - x$ into irreducible factors over $Z_p[x]$. Select all the irreducible polynomials in this factorization whose degree equals n. Let us say there are k of them $g_1(x), g_2(x), \ldots, g_k(x)$.

ii) From the $g_i's$ in (i) select those $g_i(x)$ which are primitive . We can develop the Galois field using any of these irreducible polynomials $g_i(x)$. However picking a primitive $g_i(x)$ gives a better description of the field for computational purposes . It actually provides a primitive element (a cyclic generator) for the field . From now on we will work with primitive irreducible polynomials .

iii) Suppose we have chosen a primitive irreducible polynomial of degree n from (ii). Let us call this selection $g(x)$. If we cannot decide on a primitive one , we can simply pick any $g_i(x)$ from (ii) .

iv) Let $F = \{ f(x) \in Z_p[x] : \text{degree of } f(x) \leq n - 1 \}$, i.e. F is the set of polynomials of the form $a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1}$ with $a_i \in Z_p$. Let $f_1(x)$, $f_2(x)$ be in F. To add $f_1(x)$ and $f_2(x)$, we do term by term addition of polynomials reducing the coefficients mod p. To multiply $f_1(x)$

with $f_2(x)$ we do the usual multiplication reducing the coefficients mod p. Then we divide this product by $g(x)$, where $g(x)$ is chosen in (iii) , and take the remainder as the product of f_1 with f_2 . We call this procedure of adding and multiplying mod$(p, g(x))$ *arithmetic* .

v) The set F defined under mod$(p, g(x))$ arithmetic is a Galois field of order p^n . To verify this , we refer to Herstein (1996) .

Consider a Galois field $GF(s)$ of order s, where $s = p^n$, with p an odd prime . An element $a \in GF(s)$ is called a *quadratic residue* (for short QR) if and only if there exists some $b \in GF(s)$ such that $a = b^2$. If no such b exists `$a$` is called a *quadratic nonresidue*. Note that 0 , 1 are always quadratic residues of $GF(s)$.

Let x be a primitive element of the multiplicative group $F^* = F - \{0\}$, where F is a $GF(s)$, $s = p^n$, p is an odd prime . Then all the quadratic residues of F are in the set $QR = \{ x^0, x^2, x^4, \ldots, x^{s-3} \}$.

We illustrate the steps (i) - (v) by developing some examples of Galois fields which will be useful later in this paper .

Example 3.1 : We construct $F = GF(7)$. Since 7 is a prime number we take $F = Z_7 = \{ 0, 1, 2, 3, 4, 5, 6 \}$ under mod 7 addition and multiplication . The addition and multiplication tables are given below :

$+_7$	0 1 2 3 4 5 6
0	0 1 2 3 4 5 6
1	1 2 3 4 5 6 0
2	2 3 4 5 6 0 1
3	3 4 5 6 0 1 2
4	4 5 6 0 1 2 3
5	5 6 0 1 2 3 4
6	6 0 1 2 3 4 5

$*_7$	0 1 2 3 4 5 6
0	0 0 0 0 0 0 0
1	0 1 2 3 4 5 6
2	0 2 4 6 1 3 5
3	0 3 6 2 5 1 4
4	0 4 1 5 2 6 3
5	0 5 3 1 6 4 2
6	0 6 5 4 3 2 1

Note that 3 is a primitive element of F and
$QR = \{ 0, 3^0, 3^2, 3^4 \} = \{ 0, 1, 2, 4 \}$.

Example 3.2 : We construct $GF(9)$. Note that $9 = 3^2$, so the base prime is 3 and the basic Galois field we work with is Z_3. Factorize $x^9 - x$ into irreducible polynomials over $Z_3[x]$:

$x^9 - x = x(x^8 - 1) = x(x^4 - 1)(x^4 + 1) = x(x - 1)(x + 1)(x^2 + 1)(x^2 + 2x + 2)(x^2 + x + 2)$

By Theorem 3.2.2 , the remainder theorem , the polynomials $g_1(x) = x^2 + 1$, $g_2(x) = x^2 + 2x + 2$, and $g_3(x) = x^2 + x + 2$ are irreducible. Of these the polynomial $g_1(x)$ is not primitive since $x^2 + 1 \mid x^4 - 1$. From the factorization of $x^9 - x$ it is clear the polynomials $g_2(x)$ and $g_3(x)$ are both primitive irreducible polynomials . We will work with $g_2(x)$.

Consider the set $F = \{ a_0 + a_1 x : a_0, a_1 \in Z_3[x] \}$, under $\bmod(3, g_2(x))$ arithmetic . Then F has the nine elements as follows :

$$\left.\begin{array}{ll} a_0 = 0, & a_1 = 0 \\ & a_1 = 1 \\ & a_1 = 2 \end{array}\right\} : \begin{array}{l} 0 \\ x, \\ 2x \end{array} \qquad \left.\begin{array}{ll} a_0 = 1, & a_1 = 0 \\ & a_1 = 1 \\ & a_1 = 2 \end{array}\right\} : \begin{array}{l} 1 \\ 1+x, \\ 1+2x \end{array}$$

$$\left.\begin{array}{ll} a_0 = 2, & a_1 = 0 \\ & a_1 = 1 \\ & a_1 = 2 \end{array}\right\} : \begin{array}{l} 2 \\ 2+x \\ 2+2x \end{array}$$

By Theorem 3.3 (ii) ,

$F^* = F - \{0\} = \{ 1, x, 1+x, 2x, 1+2x, 2, 2+x, 2+2x \}$ is a cyclic group under multiplication , and x is a primitive element (generator) for F^*. To verify this we calculate sucessive powers of x, using $\bmod(3, g_2(x))$ arithmetic to get:

0, $x^0 = 1$, $x^1 = x$, $x^2 = x + 1$ (replacing x^2 by $x + 1$),

$x^3 = x^2 + x = x + 1 + x = 2x + 1$,

$x^4 = x(2x + 1) = 2x^2 + x = 2x + 2 + x = 2$,

$x^5 = 2x$, $x^6 = 2x^2 = 2(x + 1) = 2x + 2$,

$x^7 = 2x^2 + 2x = 2x + 2 + 2x = x + 2$,

$x^8 = x^2 + 2x = x + 1 + 2x = 1$. Thus the powers of x generate F^*, and x is a primitive element of F^*.

Let us summarize our construction . The elements of F are

$F = \quad 0, 1, x, x^2, x^3, x^4, x^5, x^6, x^7 \qquad 0, 1, x, x \quad 1, 2x \quad 1, 2, 2x, 2x \quad 2, x \quad 2$

The mod $(3, g_2(x))$ arithmetic tables , one for addition and the other for multiplication are as follows :

$+_3$	0	1	x	x+1	2x+1	2	2x	2x+2	x+2
0	0	1	x	x+1	2x+1	2	2x	2x+2	x+2
1	1	2	x+1	x+2	2x+2	0	2x+1	2x	x
x	x	x+1	2x	2x+1	1	x+2	0	2	2x+2
x+1	x+1	x+2	2x+1	2x+2	2	x	1	0	2x
2x+1	2x+1	2x+2	1	2	x+2	2x	x+1	x	0
2	2	0	x+2	x	2x	1	2x+2	2x+1	x+1
2x	2x	2x+1	0	1	x+1	2x+2	x	x+2	2
2x+2	2x+2	2x	2	0	x	2x+1	x+2	x+1	1
x+2	x+2	x	2x+2	2x	0	x+1	2	1	2x+1

$+_3, *_3$	0	1	x	x+1	2x+1	2	2x	2x+2	x+2
0	0	0	0	0	0	0	0	0	0
1	0	1	x	x+1	2x+1	2	2x	2x+2	x+2
x	0	x	x+1	2x+1	2	2x	2x+2	x+2	1
x+1	0	x+1	2x+1	2	2x	2x+2	x+2	1	x
2x+1	0	2x+1	2	2x	2x+2	x+2	1	x	x+1
2	0	2	2x	2x+2	x+2	1	x	x+1	2x+1
2x	0	2x	2x+2	x+2	1	x	x+1	2x+1	2
2x+2	0	2x+2	x+2	1	x	x+1	2x+1	2	2x
x+2	0	x+2	1	x	x+1	2x+1	2	2x	2x+2

From the above presentation the quadratic residue set in $GF(9)$ is

$QR = \{ \ 0, \ x^0, \ x^2, \ x^4, \ x^6 \ \} = \{ \ 0, 1, x+1, 2, 2x+2 \ \}$.

Example 3.3 : We construct $F = GF(11)$. Since 11 is a prime number we take $F = Z_{11} = \{ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 \}$ under mod 11 arithmetic . The mod 11 addition and multiplication tables are as follows:

$+_{11}$	0	1	2	3	4	5	6	7	8	9	10
0	0	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10	0
2	2	3	4	5	6	7	8	9	10	0	1
3	3	4	5	6	7	8	9	10	0	1	2
4	4	5	6	7	8	9	10	0	1	2	3
5	5	6	7	8	9	10	0	1	2	3	4
6	6	7	8	9	10	0	1	2	3	4	5
7	7	8	9	10	0	1	2	3	4	5	6
8	8	9	10	0	1	2	3	4	5	6	7
9	9	10	0	1	2	3	4	5	6	7	8
10	10	0	1	2	3	4	5	6	7	8	9

$*_{11}$	0	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10
2	0	2	4	6	8	10	1	3	5	7	9
3	0	3	6	9	1	4	7	10	2	5	8
4	0	4	8	1	5	9	2	6	10	3	7
5	0	5	10	4	9	3	8	2	7	1	6
6	0	6	1	7	2	8	3	9	4	10	5
7	0	7	3	10	6	2	9	5	1	8	4
8	0	8	5	2	10	7	4	1	9	6	3
9	0	9	7	5	3	1	10	8	6	4	2
10	0	10	9	8	7	6	5	4	3	2	1

Note that 2 is a primitive element in $GF(11)$. Thus

$$QR = \{ 0, 2^0, 2^2, 2^4, 2^6, 2^8 \} = \{ 0, 1, 3, 4, 5, 9 \}.$$

Example 3.4 : To construct $F = GF(19)$, since 19 is a prime number then we take

$F = Z_{19} = \{ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18 \}$ under mod 19 arithmetic . The addition and multiplication tables may be constructed on the same principles as in Example 3.2.3 . Note that 3 is a primitive element mod 19 and the set of quadratic residues in F is $QR = \{ 1, 4, 5, 6, 7, 9, 11, 16, 17 \}$.

Example 3.5 : Suppose that the problem is to determine the quadratic residues and quadratic nonresidues in the Galois field $GF(25)$.

i) First we determine a quadratic primitive irreducible polynomial over Z_5. To this end we take the factor $x^{12}+1$ in the factorization $x^{24}-1 = (x^{12}-1)(x^{12}+1)$, and factorize it into irreducible factors over Z_5 (remember that the arithmetic on the coefficients is done mod 5) :

$$x^{12}+1 = (x^4)^3 + 1^3 = (x^4+1)(x^8 - x^4 + 1) .$$

Now

$$x^4+1=(x^2+2)(x^2+3),$$

$$x^8-x^4+1=(x^4+4)^2-(2x^2)^2=(x^4-2x^2+4)(x^4+2x^2+4)$$

$$x^4-2x^2+4=(x^2+2)^2-x^2=(x^2+x+2)(x^2-x+2)$$

$$x^4+2x^2+4=(x^2+3)^2-(2x)^2=(x^2+2x+3)(x^2-2x+3)$$

Thus

$$x^{12}+1=(x^2+2)(x^2+3)(x^2+x+2)(x^2-x+2)(x^2+2x+3)(x^2-2x+3)\ .$$

ii) Now $x^4+1=(x^2+2)(x^2+3)$ divides x^8-1 . Hence neither $g_1(x)=x^2+2$ nor $g_2(x)=x^2+3$ are primitive irreducible polynomials over Z_5. However, each of $g_3(x)=x^2+x+2$, $g_4(x)=x^2-x+2$, $g_5(x)=x^2+2x+3$ or $g_6(x)=x^2-2x+3$ are primitive irreducible polynomials over Z_5. Any of these may be used to develop $GF(25)$ giving both a multiplicative and additive representation to the elements of $GF(25)$. If either $g_1(x)$ or $g_2(x)$ is used we would obtain the additive representations of the elements of $GF(25)$ under mod$(5,\ g_i(x))$ arithmetic, $i=1,\ 2$, but not the multiplicative representation .

iii) Suppose we select $g(x)=g_3(x)=x^2+x+2$ to develop $GF(25)$. Then under mod$(5,\ x^2+x+2)$ arithmetic the set

$$F=\{x^i\ ;\ 0\le i\le 23\}\cup\{0\}$$

$$=\{\ ax+b\ :\ \ a\ ,\ b\in Z_5\ \}$$

is a Galois field of order 25 . Below we tabulate the elements of F in their multiplicative and additive form :

0	1	x	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9	x^{10}
0	1	x	$4x+3$	$4x+2$	$3x+2$	$4x+4$	2	$2x$	$3x+1$	$3x+4$	$x+4$

x^{11}	x^{12}	x^{13}	x^{14}	x^{15}	x^{16}	x^{17}	x^{18}	x^{19}	x^{20}	x^{21}	x^{22}	x^{23}
$3x+3$	4	$4x+4$	$x+2$	$x+3$	$2x+3$	$x+1$	3	$3x+2$	4	$2x+1$	$4x+1$	$2x+2$

iv) From the table in (iii): the quadratic residues in $GF(25)$ is the set

$QR=\{\ 0\ ,\ 1\ ,\ 4x+3\ ,\ 3x+2\ ,\ 2\ ,\ 3x+1\ ,\ x+4\ ,\ 4\ ,\ x+2\ ,\ 2x+3\ ,\ 3\ ,\ 2x+4\ ,\ 4x+1\ \}$.

The quadratic nonresidues in $GF(25)$ is the set

$\{\ x\ ,\ 4x+2\ ,\ 4x+4\ ,\ 2x\ ,\ 3x+4\ ,\ 3x+3\ ,\ 4x\ ,\ x+3\ ,\ x+1\ ,\ 3x\ ,\ 2x+1\ ,\ 2x+2\ \}$.

Remarks :

a) It is interesting to note that in Example 3.5, 2 and 3 are quadratic nonresidues in $Z_5 = GF(5)$ but are quadratic residues in $GF(25)$.

b) One can establish that there are exactly $\frac{(p^2 - p)}{2}$ monic irreducible quadratic polynomials over Z_p , p a prime . For the case $p = 5$, there are thus $\frac{(25 - 5)}{2} = 10$ monic irreducible quadratic polynomials over Z_5. Six of these are given in (ii) of Example 3.5 . The remaining four of these monic irreducible quadratic polynomials appear as factors of $x^{12} - 1$:

$$x^{12} - 1 = (x^6 - 1)(x^6 + 1)$$

$$= (x - 1)(x + 1)(x + 2)(x + 3)(x^2 + x + 1)(x^2 - x + 1)(x^2 + 2x + 4)(x^2 - 2x + 4) .$$

Of course none of these four monic irreducible quadratic polynomials are primitive since each divides $x^{12} - 1$.

4. Paley's Constructions

Firstly, we have shown that for the even prime $p = 2$ and any positive integer k a Hadamard matrix of order $n = 2^k$ may be constructed by repeatedly taking the Kronecker product of $H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ with itself k times . This raises the question of the construction of Hadamard matrices whose order n is related to an odd prime power. In this connection Paley (1933) offered the following two constructions :

(P1) a Hadamard matrix of order $n = s + 1$ can be constructed where s is a prime power , say $s = p^r$, p a prime and $s \equiv 3 \pmod 4$.

(P2) a Hadamard matrix of order $n = 2(s + 1)$ can be constructed, where $s = p^r$ is a power of a prime p and $s \equiv 1 \pmod 4$.

The purpose of this part is to develop and present the Paley constructions outlined in (P1) and (P2) . Both involve the use of Galois fields $GF(s)$. Unlike the Kronecker product construction which requires at least one pre-existing Hadamard matrix to implement it , the Paley

construction produces a Hadamard matrix once the order of the matrix is specified as in (P1) or (P2) .

The following notation and setting will be used in the formulation of the results below. Let $F = GF(s)$ be a Galois field of order s where $s = p^r$ and p is an odd prime number. Let $H = \{1,-1\}$ be the two element multiplicative subgroup of the multiplicative group of the nonzero real numbers . Recall that the set of nonzero elements of F , call it F^*, is a cyclic group under multiplication . The following mapping χ, known as a *character* , and some of its properties will be helpful in detailing the Paley constructions : $\chi : F^* \to H$ is the mapping defined by

$$\chi(a) = \begin{cases} 1, & a \text{ is a quadratic residue in } F^* , \\ -1, & a \text{ is a quadratic nonresidue in } F^* . \end{cases}$$

Lemma 4.1 : The character $\chi : F^* \to H$ is a group homomorphism between the two multiplicative groups .

Proof : Note that the product of two nonzero quadratic residues or the product of two quadratic nonresidues is a quadratic residue , whereas the product of a nonzero quadratic residue and a quadratic nonresidue is a quadratic nonresidue . From this it is immediate that $\chi(a\,b) = \chi(a)\,\chi(b)$ for all a , b in F^* and the lemma is established. □

Corollary 4.1 : In F there are precisely $\frac{s+1}{2}$ quadratic residues and $\frac{s-1}{2}$ quadratic nonresidues . Moreover $\sum_{a \in F^*} \chi(a) = 0$.

Proof : From Lemma 4.1 , the kernel of χ consists of the quadratic residues in F^* and the only other coset of χ consists of the quadratic nonresidues . Since the cardinality of F^* , $|F^*| = s-1$, it follows that F^* has $\frac{s-1}{2}$ quadratic residues and $\frac{s-1}{2}$ quadratic nonresidues . Since the zero element 0 in F is also a quadratic residue the total number of quadratic residues in F is $\frac{s+1}{2}$ and the corollary is established . □

Lemma 4.2 :

i) When $s = p^r \equiv 1 \pmod 4$ then -1 is a quadratic residue in F.

ii) When $s = p^r \equiv 3 \pmod 4$ then -1 is a quadratic nonresidue in F.

Proof : Let x be a primitive element (generator) of the cyclic group F^*. Since the order of F^* is $s-1$ we conclude that $x^{s-1} = 1$. Hence $(x^{(s-1)/2} - 1)(x^{(s-1)/2} + 1) = 0$. Since F is a field and the order of x is $s-1$ we conclude that $x^{(s-1)/2} + 1 = 0$ or $x^{(s-1)/2} = -1$. When $s \equiv 1 \pmod 4$ then $s = 4k+1$ for some integer k. Then $x^{(s-1)/2} = x^{2k} = (x^k)^2 = -1$ and -1 is a quadratic residue establishing (i) . When $s \equiv 3 \pmod 4$ then $s = 4m+3$ for some integer m. Then $x^{(s-1)/2} = x^{2m+1} = -1$ and x is a quadratic nonresidue establishing (ii) . □

Corollary 4.2 :

i) When $s = p^r \equiv 1 \pmod 4$ then $\chi(-a) = \chi(a)$ for all a in F^*.

ii) When $s = p^r \equiv 3 \pmod 4$ then $\chi(-a) = -\chi(a)$ for all a in F^*.

Proof : Using Lemma 4.1 , for any $a \in F$ we have $\chi(-a) = \chi((-1)(a)) = \chi(-1)\chi(a)$. When $s \equiv 1 \pmod 4$, $\chi(-1) = 1$ and when $s \equiv 3 \pmod 4$, $\chi(-1) = -1$ by Lemma 4.2 and the definition of χ. From this both (i) and (ii) follow completing the proof . □

In the following it will be useful to extend the definition of the character χ to all of F by placing $\chi(0) = 0$, where the first 0 is the zero element of F and the second zero is the real number 0 . With this extended definition we have χ as a map from F to the set $\{-1,0,1\}$. The following lemma will be most helpful in establishing our first main result .

Lemma 4.3 : $\sum_{b \in F} \chi(b)\chi(b+c) = -1$, if $c \neq 0$.

Proof : $\chi(0)\ \chi(0+c) = 0$ .Since F is a field , when $b \neq 0$, b^{-1} exists . Let $z = b^{-1}(b+c)$. Then $z \neq 0$ when $b \neq -c$, and z is the *unique* element in F such that $bz = b + c$. Let $K = \{\, z = b^{-1}(b+c) \ : b \in F^*, b \neq -c \,\}$. We note that $K = F^* - \{1\}$, where 1 is the unit element of F. Note that $b^{-1}(b+c) \neq 1$ for any $b \in F^*$, for otherwise $b + c = b$ from which $c = 0$, a contradiction .

Hence $K \subseteq F^* - \{1\}$. Next , let $x \in F^* - \{1\}$. Define $b = c(x-1)^{-1}$. Then $b \neq 0$, for otherwise $c = 0$ or $x = 1$, neither of which is the case . Moreover $b^{-1}(b+c) = c^{-1}(x-1)[c(x-1)^{-1} + c] = 1 + (x-1) = x$ from which we conclude that $x \in K$. Hence $F^* - \{1\} \subseteq K$. In all $K = F^* - \{1\}$. Now ,

$\sum_{b \in F} \chi(b)\chi(b+c) = \sum_{b \in F^*} \chi(b)\chi(b+c) = \sum_{z \in F^* - \{1\}} \chi(b)\chi(bz)$, since

$K = F^* - \{1\}$. By Lemma 4.1, $\chi(bz) = \chi(b)\chi(z)$ and thus

$\sum_{b \in F} \chi(b)\chi(b+c) = \sum_{z \in F^* - \{1\}} [\chi(b)]^2 \chi(z) = \sum_{z IN F^* - \{1\}} \chi(z) = \sum_{z \in F^*} \chi(z) - \chi(1) = 0 - 1 = -1$,

using Corollary 4.1 . □

A real matrix M of order n is called *skew symmetric* if and only if $M = -M'$. It is clear that any skew symmetric matrix has each of its diagonal entries equal to zero. Recall that a Hadamard matrix H of order n is called a *skew Hadamard* matrix if and only if $H = I_n + S$, where S is a skew symmetric matrix . Clearly to obtain a skew Hadamard matrix we need a skew symmetric matrix whose off diagonal entries are +1 or -1.

We now introduce a matrix Q of order $s = p^r$, p an odd prime , and study its properties in the lemmas below . This matrix Q will play a crucial role in both Paley constructions. The definition of Q is based on the Galois field F of order $s = p^r$, p an odd prime and uses the character χ defined on F : let $F = \{ \alpha_- , \alpha_1 , \alpha_2 , \ldots , \alpha_{s-1} \}$ be a listing of the s elements of F with $\alpha_- = 0$. Define

$$Q = (q_{ij})_{sxs} \quad , \quad q_{ij} = \chi(\alpha_j - \alpha_i) \qquad (3.1)$$

Lemma 4.4 : The matrix Q is a matrix with entries in the set $\{-1,0,1\}$. When $s = p^r \equiv 1 \pmod 4$ then Q is a symmetric matrix . When $s = p^r \equiv 3 \pmod 4$ then Q is a skew symmetric matrix .

Proof : The first statement of the lemma follows from the definition of the character χ .

Moreover

$$q_{ij} = \chi(\alpha_j - \alpha_i) = \chi((-1)(\alpha_i - \alpha_j)) = \begin{cases} -\chi(\alpha_i - \alpha_j), \text{when } p^r \equiv 3 \pmod 4, \\ \chi(\alpha_i - \alpha_j), \text{when } p^r \equiv 1 \pmod 4, \end{cases}$$

$$= \begin{cases} -q_{ji}, \text{when } p^r \equiv 3 \pmod 4, \\ q_{ji}, \text{when } p^r \equiv 1 \pmod 4, \end{cases}$$

using Corollary 4.2 . This completes the proof . □

The following notation will be useful and will be employed throughout : J_{mxn} will denote a matrix of order mxn each of whose entries is +1 . We simply write J when its dimension is apparent from the context.

Lemma 4.5 : Q satisfies the following :

i) $QQ' = s\,I_s - J$,

ii) $Q\,J = J\,Q = 0$,

Proof :

i) Let $Q'Q = B = (b_{ij})$, then

b_{ij} = inner product of the i-th row of Q with the j-th row of Q

$= \sum_k q_{ik}\ q_{jk} = \sum_k \chi(\alpha_k - \alpha_i)\,\chi(\alpha_k - \alpha_j) = s - 1$ if $i = j$, and equals -1 if $i \neq j$ using Lemma 4.3 and taking $b = \alpha_k - \alpha_i$ and $c = \alpha_i - \alpha_j \neq 0$ in that lemma . This establishes (i).

ii) $QJ = 0$ follows from $\sum_j \chi(\alpha_i - \alpha_j) = 0$ using Corollary 4.1 . □

We now use the matrix Q defined in (3.1) , to define the following matrix which is of major importance in the Paley constructions :

$$S = \begin{pmatrix} 0 & -J_{1xs} \\ J_{sx1} & Q \end{pmatrix}_{(s+1)x(s+1)} \qquad (3.2)$$

Lemma 4.6 : Let $s = p^r$, p an odd prime , with $p \equiv 3 \pmod 4$. Then the matrix S defined in (3.2) has the properties :

i) $S' = -S$, namely S is skew symmetric ,

ii) $S'S = s\,I_{s+1}$.

Proof :

i) This follows from Lemma 4.4 , since Q is skew symmetric when $p \equiv 3 \pmod 4$.

ii) $$SS' = \begin{pmatrix} 0 & -J_{1\times s} \\ J_{s\times 1} & Q \end{pmatrix}\begin{pmatrix} 0 & J_{1\times s} \\ -J_{s\times 1} & Q' \end{pmatrix} = \begin{pmatrix} s & \underline{0}' \\ \underline{0} & QQ' + J_{s\times s} \end{pmatrix} = sI_{s+1},$$

using Lemma 4.5 (i). This completes the proof . □

We are now ready to give the first Paley construction (the construction outlined in statement (P1)) .

Theorem 4.1 : [The First Paley construction ; Paley (1933)]

Let $s = p^r$, p an odd prime , with $p \equiv 3 \pmod 4$. Then the matrix $H_{s+1} = I_{s+1} + S$, where S is defined as in (3.2) is a skew Hadamard matrix of order $s+1$.

Proof :

$H'H = (I+S)(I+S') = I + S + S' + S\,S' = I + S - S + s\,I_{s+1} = (s+1)\,I_{s+1}$, using Lemma 4.6 . Hence H is a skew Hadamard matrix of order $s+1$. This completes the proof . □

We illustrate Theorem 4.1 by constructing a Hadamard matrix of order 28 . This presented in the following example .

Example 4.1 : To make the presentation self contained we recall some definitions from the second part of this paper . In addition we will require the Remainder Theorem [Theorem 3.2] and two other theorems quoted below ; the proofs of the latter two theorems may be found in any standard book on abstract algebra which discusses Galois fields, for example, Herstein (1996) .

Throughout p will denote a prime, $n \geq 1$ will be an integer and let $s = p^n$.

A polynomial $f(x)$ in the polynomial ring $Z_p[x]$ will be called *reducible* iff $f(x) = g_1(x)\,.\,g_2(x)$ for some $g_i \in Z_p[x]$ with degree g_i < degree f for $i = 1, 2$ .Otherwise f is called *irreducible.* Moreover, $f(x)$ is called *monic* iff the coefficient of its highest degree term is 1 . An irreducible polynomial

$f(x)$ in $Z_p[x]$ is called *primitive* iff $f(x)$ divides the polynomial $x^m - 1$ for $m = s - 1$ but does not divide $x^m - 1$ for any m such that $1 \le m < s - 1$.

The importance of irreducible polynomials stems from the following :

(GF1) let $g(x)$ in $Z_p[x]$ be any monic irreducible polynomial of degree n ,

(GF2) let $F = \{ \quad f(x) \quad : \quad f(x) \in Z_p[x] \quad , \text{degree } f(x) \le n - 1 \quad \}$.

Then the underlying set F under mod$(\ p\ ,\ g(x))$ arithmetic is a Galois field of order s . We write $GF(s)$ as a shorthand for the Galois field of order s and it denotes the pair $(\ F\ ,\ \text{mod}(\ p\ ,\ g(x)))$ where $g(x)$ is defined in (GF1) and F in (GF2).

Let $F^* = F - \{0\}$. We have mentioned in the second part that F^* is a cyclic group under the multiplication in F . The importance of monic irreducible primitive polynomials is due to the following :

(GF4) if the monic irreducible polynomial $g(x)$ in (GF1) is also primitive then the cyclic group F^* is generated by the polynomial $q(x) = x$ in F under mod$(\ p\ ,\ g(x))$ arithmetic . In fact F^* has $\phi(s - 1)$ generators, where ϕ is the Euler ϕ - function, and $F^* = \{ \quad x^i \quad : \quad 0 \le i \le s - 2 \quad \}$. Thus $x^t \in F^*$ is also a generator of F^* iff

$t \le s - 1$ and t is relatively prime to $s - 1$.

The above discussion raises two questions :

Question 1 : How does one find monic irreducible polynomials $g(x)$ in $Z_p[x]$ of degree n ?

Question 2 : How does one find monic irreducible primitive polynomials in $Z_p[x]$ of degree n ?

Let us consider the special polynomial $Q_s(x) = x^s - x$. An answer to both questions can be given in terms of factorizing $Q_s(x)$ in $Z_p[x]$. The answer is not too satisfactory, as we shall see, because often $Q_s(x)$ is very difficult to factorize .

Theorem A : (i) Let $g(x)$ be any monic irreducible polynomial of degree dividing n . Then $g(x)$ divides $Q_s(x)$.

(ii) The polynomial $Q_s(x)$ equals the product of all monic irreducible polynomials whose degrees divide n .

(iii) The number of monic irreducible polynomials of degree n is equal to $\frac{[\phi(s-1)]}{n}$ where ϕ is the Euler ϕ-function .

The next result reduces the labour involved in checking that an irreducible polynomial of degree n is primitive in certain cases .

Theorem B : Suppose that $p \equiv 3 \pmod 4$. Let $g(x)$ be a monic irreducible polynomial of degree n . Consider the Galois field $GF(s) = (F, \text{mod}(p, g(x))$. Then,

if $x^{(s-1)/2} = -1$ under $\text{mod}(p, g(x))$ arithmetic then $g(x)$ is primitive .

We are now ready to construct H_{28} using the first Paley method . We give the construction procedure in steps . In this construction we need to develop $GF(3^3)$ so that $n = p = 3$ and $s = 27$.

Step 1. Find a cubic monic primitive irreducible polynomial in $Z_3[x]$. At first glance this step seems easy . According to Theorem A we need to factorize $Q_3(x) = x^{27} - x$ into irreducibles of degree dividing 3 . The polynomial we seek is among the factors . Now $x^{27} - x = x(x^{13} - 1)(x^{13} + 1)$ and by the Remainder Theorem $x^{13} - 1$ and $x^{13} + 1$ have $x - 1$ and $x + 1$ as factors respectively . Upon division by $x - 1$ and $x + 1$ we are left with two lengthy 12 degree polynomials which are indeed very difficult to factorize . So we abandon this approach and try a different strategy .

This strategy works well when n is small and prime . We now present the strategy as a sequence of problems and solutions .

A cubic monic polynomial in $Z_3[x]$ has the form : $a + b\,x + c\,x^2 + x^3$ with a , b , c in Z_3 . Hence there are precisely 27 such polynomials .

Problem 1 . Find all the cubic monic reducible polynomials in $Z_3[x]$.

Solution . Using the Remainder Theorem it may be verified that the list of 19 monic cubic polynomials are all reducible :

(i) $x^3 - x;\quad x^3 + x;\quad x^3 + x^2;\quad x^3 - x^2;\quad x^3 - x^2 - x;\quad x^3 + x^2 - x;\quad x^3 - x^2 + x;\quad x^3 + x^2 + x;\quad x^3$,

(ii) $x^3 - 1;\quad x^3 + x^2 + 1;\quad x^3 + x + 1;\quad x^3 - x^2 - x + 1;\quad x^3 - x^2 + x - 1;\quad x^3 + x^2 - x - 1$,

(iii) $x^3 + 1;\quad x^3 - x^2 - 1;\quad x^3 + x^2 + x + 1;\quad x^3 + x - 1$.

In fact $q(x)$ is in (i) iff $q(0) = 0$; $q(x)$ is in (ii) iff $q(1) = 0$ and $q(x)$ is in (iii) iff $q(2) = 0$.

Problem 2 . Find all the cubic monic irreducible polynomials in $Z_3[x]$.

Solution. The purpose of Problem 1 was to eliminate the 19 Monic reducible polynomials of the possible 27 monic cubic polynomials . The remaining 8 must be monic irreducible and hence any of them is suitable to develop $GF(3^3)$. We list the 8 in 2 groups :

(PI) $x^3 - x - 2;\quad x^3 - x^2 - 2;\quad x^3 + x^2 - x + 1;\quad x^3 - x^2 + x + 1$,

(NPI) $x^3 - x^2 - x - 1;\quad x^3 - x - 1;\quad x^3 + x^2 + x - 1;\quad x^3 + x^2 - 1$.

Again the Remainder Theorem may be used to verify that the 8 polynomials listed in (PI) and (NPI) are irreducible .

Problem 3. [This problem addresses Step 1] . Find a monic cubic primitive irreducible polynomial in $Z_3[x]$.

Solution. The polynomial we seek is among the 8 polynomials listed in the solution to Problem 2 . By Theorem A (iii) there are $\frac{\phi(26)}{3} = \frac{12}{3} = 4$ such cubic primitive irreducibles .

There is no quick method of identifying which 4 amongst the 8 are primitive . We resort to a well known mathematical technique : trial and error . We simply pick one of the 8 listed polynomials and apply Theorem B to it and continue on until we are succesful . In this way we find that the 4 polynomials listed in the group (PI) are primitive and the remaining 4 are not. As an illustration let us verify that the irreducible polynomial $g(x) = x^3 - x - 2$ is primitive. Consider $GF(3^3)$ under mod $(3\ ,\ g(x))$ arithmetic . Then under this arithmetic we have the *reduction relation*

(RR) : $x^3 = x + 2$

Now under mod $(3\ ,\ g(x))$ arithmetic we have

$$\begin{aligned} x^{12} = (x^3)^4 &= (x+2)^4 \text{ using (RR)} \\ &= x^4 + 2x^3 + 2x + 1 \quad \text{, expanding} \\ &= x(x+2) + 2(x+2) + 2x + 1 \text{ using (RR)} \\ &= x^2 + 2 \end{aligned}$$

Hence $x^{13} = x(x^2 + 2) = x^3 + 2x = x + 2 + 2x$ using (RR) .

$= 2 = -1$,

That is, $x^{13} = -1$ and by Theorem B, $g(x)$ is primitive .

The next problem is now unnecessary but it illustrates Theorem A .

Problem 4. Factorize $Q_s(x) = x^{27} - x$ to illustrate Theorem A .

Solution. In this case $n = 3$. Thus the only irreducibles of degree

Dividing $n = 3$ are of degree 1 or 3 . Those of degree 1 are Clearly x , $x-1$, $x+1$ and those of degree 3 are listed in (PI) and (NPI) . Hence

$$x^{26}-1 = \left[\begin{array}{l} (x+1)\,(x^3-x-2)\,(x^3-x^2-2)\,(x^3+x^2-x+1)\,(x^3-x^2+x+1) \\ \\ (x-1)\,(x^3-x^2-x-1)\,(x^3-x-1)\,(x^3+x^2+x-1)\,(x^3+x^2-1) \end{array} \right]$$

Indeed the factors in the first line multiply out to $x^{13}+1$ and those in the second line multiply out to $x^{13}-1$

Step 2. Select a monic cubic primitive irreducible polynomial and use it to develop $GF(3^3)$. Write the elements of F in both the additive form and as powers of its cyclic generator x .

This is the second crucial step in the construction process . We choose the cubic primitive irreducible polynomial $g(x) = x^3 - x - 2$. The underlying set F of $GF(3^3)$ is then $F = \{\ a x^2 + b x + c \ : \ a\ ,\ b\ ,\ c \in Z_3 \ \}$, and F under mod $(3\ ,\ g(x) = x^3 - x - 2)$ arithmetic is a Galois field of order 27. To facilitate computation under mod$(3\ ,\ g(x))$ arithmetic we will, as before, use the reduction relation :

$$\text{(RR)} : \quad x^3 = x + 2 \ .$$

Since $g(x)$ is primitive the cyclic group $F^* = F - \{0\}$ has x as a generator . Hence $F^* = \{\ x^i \ : \ 0 \le i \le 25 \ \}$. For convenience, we rename the 27 elements of F as follows:

$\alpha_{-1} = 0$ (zero element of F) , $\alpha_{\_} = x^{\infty} = 1$ (unit element of F) , and in general $\alpha_i = x^i$, $0 \le i \le 25$. Before we develop the additive (polynomial) and power form for each element of F , a very crucial step for the Paley construction, let us demonstrate a particular calculation by finding the additive form of $x^5 \in F^*$. We use (RR) as often as necessary. Now $x^5 = x^2(x^3) = x^2(x+2) = x^3 + 2x^2 = x + 2 + 2x^2 = 2x^2 + x + 2$. Thus the additive form of x^5 is $2x^2 + x + 2$. Using this method we can develop the additive form of each x^i . Since $g(x)$ is primitive, we are guaranteed that we can do 26 such calculations in succession and thereby exhaust F^* obtaining the additive form of each element of F . In the table below we record the 27 elements of F in their additive and power forms and identify each with the appropriate symbol α_i .

Elements of F in the additive and power form		
$\alpha_{-1}=0$	$\alpha_8=x^8=2x^2+2$	$\alpha_{17}=x^{17}=2x^2+x$
$\alpha_0=x^0=1$	$\alpha_9=x^9=x+1$	$\alpha_{18}=x^{18}=x^2+2x+1$
$\alpha_1=x$	$\alpha_{10}=x^{10}=x^2+x$	$\alpha_{19}=x^{19}=2x^2+2x+2$
$\alpha_2=x^2$	$\alpha_{11}=x^{11}=x^2+x+2$	$\alpha_{20}=x^{20}=2x^2+x+1$
$\alpha_3=x^3=x+2$	$\alpha_{12}=x^{12}=x^2+2$	$\alpha_{21}=x^{21}=x^2+1$
$\alpha_4=x^4=x^2+2x$	$\alpha_{13}=x^{13}=2$	$\alpha_{22}=x^{22}=2x+2$
$\alpha_5=x^5=2x^2+x+2$	$\alpha_{14}=x^{14}=2x$	$\alpha_{23}=x^{23}=2x^2+2x$
$\alpha_6=x^6=x^2+x+1$	$\alpha_{15}=x^{15}=2x^2$	$\alpha_{24}=x^{24}=2x^2+2x+1$
$\alpha_7=x^7=x^2+2x+2$	$\alpha_{16}=x^{16}=2x+1$	$\alpha_{25}=x^{25}=2x^2+1$

(T)

Step 3. Construct the Paley matrix $Q=(q_{ij})$ of order 27 defined in (3.1) of part three .

Recall that the entries q_{ij} are defined as follows :

$$q_{ij}=\begin{cases}0 \quad , \ if \ \ i=j \\ 1 \quad , \ if \ \ i\neq j \ \ and \ \ \alpha_j-\alpha_i \ \ is \ \ a \ quadratic \ residue \ in \ F \ , \\ -1 \quad , \ if \ \ i\neq j \ \ and \ \ \alpha_j-\alpha_i \ \ is \ \ a \ quadratic \ nonresidue \ in \ F \ .\end{cases}$$

The Paley matrix Q will be presented in partitioned form $Q=[\ Q_1|Q_2\ ]$, where Q_1 is of order *27x15* and Q_2 is of order *27x12* at the end of this example . The vertical and horizontal margins will be labelled by the elements α_i of F . Crucial to developing the entries of Q is table (T) of Step 2 . We illustrate how table (T) helps in developing Q by solving the next problem .

Problem 5. (i) Compute the entries $q_{4,22}$ and $q_{4,8}$ of Q.

(ii) Explain why $q_{ij}=-q_{ji}$ for all i , j .

Solution .

(i) Now $\alpha_{22}-\alpha_5=x^{22}-x^5=(2x+2)-(2x^2+x+2)=x^2+x=x^{10}$, using table

(T) twice . Since x^{10} is a quadratic residue in F , $q_{5,22} = 1$.

Similarly, $\alpha_8 - \alpha_4 = x^8 - x^4 = (2x^2 + 2) - (x^2 + 2x) = x^2 - 2x + 2 = x^{11}$, using table (T) twice . Since x^{11} is a quadratic nonresidue in F , $q_{4,8} = -1$.

(ii) Now $\alpha_j - \alpha_i = -(\alpha_i - \alpha_j)$. Also $x^{13} = -1$ from table (T) . Suppose that $\alpha_j - \alpha_i = x^k$. Then $\alpha_i - \alpha_j = -(\alpha_j - \alpha_i) = x^{13} . x^k = x^{k+13}$. Thus $k + 13$ is even iff k is odd and $k + 13$ is odd iff k is even . Hence $q_{ij} = -q_{ji}$.

Step 4 . We are now ready to construct H_{28} the Hadamard matrix of order 28 .

First we form the matrix S of order 28 defined in (3.2) of part three :

$$S = \begin{pmatrix} 0 & -J_{1x27} \\ J_{27x1} & Q \end{pmatrix},$$

where Q is the Paley matrix developed in Step 3 and J_{27x1} is a vector each of whose entries is +1 . Finally set

$$H_{28} = I_{28} + S,$$

where I_{28} is the identity matrix of order 28 . Due to Theorem 3.3.1, we know that H_{28} is a Hadamard matrix of order 28 . From Problem 5 (ii), we know that Q is skew symmetric and hence so is S . Thus by definition, the matrix H_{28} constructed here is a skew Hadamard matrix . It is interesting to note that each diagonal entry of H_{28} is +1 .

$Q_1 =$

	α_{-1}	α_0	α_1	α_2	α_3	α_4	α_5	α_6	α_7	α_8	α_9	α_{10}	α_{11}	α_{12}	α_{13}
α_{-1}	0	+	−	+	−	+	−	+	−	+	−	+	−	+	−
α_0	-	0	-	+	-	-	+	+	+	-	-	-	+	-	+
α_1	+	+	0	+	-	+	+	-	-	-	+	+	+	-	+
α_2	-	-	-	0	-	+	-	-	+	+	+	-	-	-	+
α_3	+	+	+	+	0	+	-	+	+	-	-	-	+	+	+
α_4	-	+	-	-	-	0	-	+	-	-	+	+	+	-	-
α_5	+	-	-	+	+	+	0	+	-	+	+	-	-	-	+
α_6	-	-	+	+	-	-	-	0	-	+	-	-	+	+	+
α_7	+	-	+	-	-	+	+	+	0	+	-	+	+	-	-
α_8	-	+	+	-	+	+	-	-	-	0	-	+	-	-	+
α_9	+	+	-	-	+	-	-	+	+	+	0	+	-	+	+
α_{10}	-	+	-	+	+	-	+	+	-	-	-	+	-	+	-
α_{11}	+	-	-	+	-	-	+	-	-	+	+	+	0	+	-
α_{12}	-	+	+	+	-	+	+	-	+	+	-	-	-	0	-
α_{13}	+	-	-	-	-	+	-	-	+	-	-	+	+	+	0
α_{14}	-	-	+	+	+	+	-	+	+	-	+	+	-	-	-
α_{15}	+	-	+	-	-	-	-	+	-	-	+	-	-	+	+
α_{16}	-	-	+	-	+	+	+	+	-	+	+	-	+	+	-
α_{17}	+	+	+	-	+	-	-	-	-	+	-	-	+	-	-
α_{18}	-	-	-	-	+	-	+	+	+	+	-	+	+	-	+
α_{19}	+	-	+	+	+	-	+	-	-	-	-	+	-	-	+
α_{20}	-	+	+	-	-	-	+	-	+	+	+	+	-	+	+
α_{21}	+	-	-	-	+	+	+	-	+	-	-	-	-	+	-
α_{22}	-	-	+	+	+	-	-	-	+	-	+	+	+	+	-
α_{23}	+	+	+	-	-	-	+	+	+	-	+	-	-	-	-
α_{24}	-	+	-	-	+	+	+	-	-	-	+	-	+	+	+
α_{25}	+	+	-	+	+	-	-	-	+	+	+	-	+	-	-

$Q_2 =$

	α_{14}	α_{15}	α_{16}	α_{17}	α_{18}	α_{19}	α_{20}	α_{21}	α_{22}	α_{23}	α_{24}	α_{25}
α_{-1}	+	-	+	-	+	-	+	-	+	-	+	-
α_0	+	+	+	-	+	+	-	+	+	-	-	-
α_1	-	-	-	-	+	-	-	+	-	-	+	+
α_2	-	+	+	+	+	-	+	+	-	+	+	-
α_3	-	+	-	-	-	-	+	-	-	+	-	-
α_4	-	+	-	+	+	+	+	-	+	+	-	+
α_5	+	+	-	+	-	-	-	-	+	-	-	+
α_6	-	-	-	+	-	+	+	+	+	-	+	+
α_7	-	+	+	+	-	+	-	-	-	-	+	-
α_8	+	+	-	-	-	+	-	+	+	+	+	-
α_9	-	-	-	+	+	+	-	+	-	-	-	-
α_{10}	-	+	+	+	-	-	-	+	-	+	+	+
α_{11}	+	+	-	-	-	+	+	+	-	+	-	-
α_{12}	+	-	-	+	+	+	-	-	-	+	-	+
α_{13}	+	-	+	+	-	-	-	+	+	+	-	+
α_{14}	0	-	+	-	-	+	+	+	-	-	-	+
α_{15}	+	0	+	-	+	+	-	-	-	+	+	+
α_{16}	-	-	0	-	+	-	-	+	+	+	-	-
α_{17}	+	+	+	0	+	-	+	+	-	-	-	+
α_{18}	+	-	-	-	0	-	+	-	-	+	+	+
α_{19}	-	-	+	+	+	0	+	-	+	+	-	-
α_{20}	-	+	+	-	-	-	0	-	+	-	-	+
α_{21}	-	+	-	-	+	+	+	0	+	-	+	+
α_{22}	+	+	-	+	+	-	-	-	0	-	+	-
α_{23}	+	-	-	+	-	-	+	+	+	0	+	-
α_{24}	+	-	+	+	-	+	+	-	-	-	0	-
α_{25}	-	-	+	-	-	+	-	-	+	+	+	0

We now develop the second Paley construction (outlined in statement (P2)) . This construction is based on the concept of a conference matrix . A *conference matrix* , hereafter called a *C-matrix* , is a matrix M of order n such that the diagonal entries of M are zero , the off-diagonal entries are +1 or -1 and $M'M = (n - 1) I_n$. Clearly , if M is a C-matrix then $M'M = (n - 1) I_n$ so that every pair of rows (or columns) of M are orthogonal . C-matrices were first used by Belevitch (1950) in studying the theoretical aspects of electrical networks . Later they were studied in their own right by Goethals and Seidel (1967) who in fact referred to these matrices as conference matrices . Since the second Paley construction depends on the existence of

C-matrices we state two results below without proof which shed some light on the question of their existence.

Let m be a positive integer and suppose $m = n^2 (p_1\ p_2\ p_3 \ldots\ p_k)$ where $p_i (1 \le i \le k)$ are distinct prime numbers . Then the number $t = p_1\ p_2\ p_3 \ldots\ p_k$ is called the *square free* part of m. The following two - square theorem is a well known number theoretic result and includes the celebrated two square Fermat theorem as a special case . We refer for the proof to Hardy and Wright (1954) .

Theorem 4.2 : [Two Square Theorem]

A positive integer $m = x^2 + y^2$, for some integers x and y if and only if the square free part of m consists of prime numbers each of which is congruent to $1 (\mod 4)$. The connection of the two square theorem to C-matrices occurs via the next theorem. For a proof of this next theorem see Raghavarao (1971) and Wallis et al (1972) .

Theorem 4.3 : A necessary condition for the existence of a square rational matrix M (i.e. M has rational number entries) of order $n \equiv 2 (\mod 4)$ satisfying $M'M = m I_n$ for some positive integer m is that $m = a^2 + b^2$ for some integers a and b.

A clear inference from Theorem 4.2 and 4.3 is the following :

Corollary 4.3 : A necessary condition that there exist a C-matrix of order $n \equiv 2 (\mod 4)$ is that the square free part of $n - 1$ consists of prime numbers each of which is congruent to $1 (\mod 4)$.

From Corollary 4.3 we conclude that there are many values of $n \equiv 2 (\mod 4)$ for which a C-matrix of order n does not exist . For examples C-matrices of orders $n = 22, 34, 58, 78, \ldots, etc$ .do not exist . For a listing of orders <1000 for which C-matrices exist and those orders excluded by the above results see Wallis et al (1972).

For certain $n \equiv 2 (\mod 4)$ a C-matrix of this order n always exist . Indeed the developments earlier in this part guarantees this . To ferret out this pleasant situation we adjust the definition of S given in (3.2) .

Consider the matrix T of order $s+1$ defined as follows :

$$T = T_{s+1} = \begin{pmatrix} 0 & J_{1xs} \\ J_{sx1} & Q \end{pmatrix}_{(s+1)x(s+1)} \qquad (3.3)$$

where the matrix Q is defined in (3.1) .

Lemma 4.7 : Suppose that the order $s = p^r$, p an odd prime , of the Galois field F satisfies $s \equiv 1 \pmod 4$. Let T be the matrix of order $s+1$ defined in (3.3). Then T is a symmetric C-matrix .

Proof : Since $s \equiv 1 \pmod 4$, Q is symmetric by Lemma 4.4 and hence so is T . Further , as in the proof of Lemma 4.6 ,

$T'T = \begin{pmatrix} s & \underline{0'} \\ \underline{0} & QQ' + J_{sxs} \end{pmatrix} = s\, I_{s+1}$, using Lemma 4.5 (i) . Hence T is a C-matrix , completing the proof . □

We remark that the matrix S of order $s+1$ defined in (3.2) is also a C-matrix but it is not symmetric . The second Paley construction requires a symmetric C-matrix and this necessitates the adjustment of S to T as done in (3.3) .

Example 4.2 : We construct the symmetric C-matrix T_6. First $GF(5) = \{0, 1, 2, 3, 4\}$ under $+_5$, $*_5$. The quadratic residues of $GF(5)$ is the set $QR = \{0, 1, 4\}$ and the quadratic nonresidues is the set $\{2, 3\}$. Thus

$$Q = \begin{pmatrix} 0 & + & - & - & + \\ + & 0 & + & - & - \\ - & + & 0 & + & - \\ - & - & + & 0 & + \\ + & - & - & + & 0 \end{pmatrix}_{5x5} \quad \text{and} \quad T_6 = \begin{pmatrix} 0 & + & + & + & + & + \\ + & 0 & + & - & - & + \\ + & + & 0 & + & - & - \\ + & - & + & 0 & + & - \\ + & - & - & + & 0 & + \\ + & + & - & - & + & 0 \end{pmatrix}_{6x6} .$$

It may be verified that $T_6\ T_{6'} = T_{6'}\ T_6 = 5\, I_6$.

Example 4.3 : We construct the symmetric C-matrix T_{10}. First, as in Example 3.2, we consider
$GF(9)=\{\ 0,\ x^{-}=1,\ x^{1}=x,\ x^{2}=x+1,\ x^{3}=2x+1,\ x^{4}=2,\ x^{5}=2x,\ x^{6}=2x+2,\ x^{7}=x+2\ \}$ under mod $(3,\ x^{2}+2x+2)$ arithmetic . The set of quadratic residues of $GF(9)$ is $QR=\{\ 0,\ 1,\ x+1,\ 2,\ 2x+2\ \}$ and the set of quadratic nonresidues is $\{\ x,\ 2x+1,\ 2x,\ x+2\ \}$. Thus the matrix $Q=(q_{ij})$ of order 9 defined in (3.1) is displayed below (the horizontal and vertical margins are indexed by the elements of $GF(9)$) :

$Q =$

	0	1	x	x+1	2 x+1	2	2 x	2 x+2	x+2
0	0	1	-1	1	-1	1	-1	1	-1
1	1	0	-1	-1	-1	1	1	-1	1
x	-1	-1	0	1	1	1	-1	-1	1
x+1	1	-1	1	0	-1	-1	-1	1	1
2 x+1	-1	-1	1	-1	0	1	1	1	-1
2	1	1	1	-1	1	0	-1	-1	-1
2 x	-1	1	-1	-1	1	-1	0	1	1
2 x+2	1	-1	-1	1	1	-1	1	0	-1
x+2	-1	1	1	1	-1	-1	1	-1	0

Then the symmetric C-matrix T_{10} defined in (3.3) is obtained from Q by bordering it as follows :

$$T_{10} = \begin{pmatrix} 0 & 1' \\ 1 & Q \end{pmatrix}_{10x10} .$$

Theorem 4.4 : [Second Paley Construction ; Paley (1933)]

i) If a symmetric C-matrix M of order n exists then the matrix

$$H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes M + \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} \otimes I_n \qquad (3.4)$$

where $\otimes$ is the Kronecker product , is a symmetric Hadamard matrix of order $2n$.

ii) If T is the symmetric C-matrix of order $s+1$ defined in (3.3) ,where $s = p^{r} \equiv 1 \pmod 4$ and p is an odd prime , then

$$H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes T + \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} \otimes I_n$$

is a symmetric Hadamard matrix of order $2s+2$.

Proof : (ii) is immediate from (i) and Lemma 4.7 . Hence we prove (i) . Note that H defined in (3.4) can be rewriten as

$$H = \begin{pmatrix} M+I & M-I \\ M-I & -(M+I) \end{pmatrix}.$$ Now by direct multiplication ,

$$HH' = \begin{pmatrix} M+I & M-I \\ M-I & -(M+I) \end{pmatrix} \begin{pmatrix} M'+I & M'-I \\ M'-I & -(M'+I) \end{pmatrix} = 2nI,$$

performing the block multiplication and using $M = M'$ and $M'M = (n-1)I_n$.

□

The Paley constructions given in Theorems 4.1 and 4.4 form the backbone of a number of further construction results on Hadamard matrices based on Galois fields which have been developed since Paley's initial effort in 1933 described here . At this point we simply summarize some of these additional construction results below . We emphasize that these are actual constructions when the stated conditions are met , as are the Paley theorems , and not merely existence statements . For detailed proofs of these results see Hall (1967) . As in first part , the constructions below are of the recursive type , and use the Kronecker product when appropriate .

Theorem 4.5 : [Williamson (1944) ; Generalization of Paley's second Construction]
If $s = p^r \equiv 1 \pmod 4$, p a prime and if a Hadamard matrix H of order $n > 1$ is given then a Hadamard matrix of order $n(s+1)$ can be constructed .

Theorem 4.6 :

i) Let $n = 2^t k_1 k_2 \dots k_m$. Suppose that either $k_i = p_i^{r_i} + 1 \equiv 0 \pmod 4$ or $k_i = 2(p_i^{r_i} + 1)$, $p_i^{r_i} \equiv 1 \pmod 4$ for each i . Then a symmetric Hadamard matrix of order n can be constructed .

ii) Let a skew Hadamard matrix of order n be given . Suppose that $s = p^r \equiv 3 \pmod 4$, where p is a prime . Then a skew Hadamard matrix of order $n(s+1)$ can be constructed .

iii) Let $n = 2^t k_1 k_2 \dots k_m$ where each $k_i = p_i^{r_i} + 1 \equiv 0 \pmod 4$ with p_i

prime . Then a skew Hadamard matrix of order n can be constructed .

iv) Let a skew Hadamard matrix of order n be given . Then a Hadamard matrix of order $n(n-1)$ can be constructed .

v) Let a skew Hadamard matrix of order n and a symmetric Hadamard matrix of order $m = n+4$ be given. Then a Hadamard matrix of order $n(n+3)$ can be constructed.

vi) Let two Hadamard matrices of orders $n_1 > 1$ and $n_2 > 1$ be given . Let p be a prime such that $p^r \equiv 1 \pmod 4$. Then a Hadamard matrix of order $n_1 n_2 (p^r + 1) p^r$ can be constructed .

vii) Let two Hadamard matrices of orders $n_1 > 1$ and $n_2 > 1$ be given . Suppose that n is a positive number such that $n = p_1^{r_1} + 1$ for some prime p_1 and $n+4 = p_2^{r_2} + 1$ for some prime p_2. Then a Hadamard matrix of order $n_1 n_2 n(n+3)$ can be constructed .

We now give some examples to illustrate the two Paley constructions .

Example 4.4 : To construct a Hadamard matrix of order 8 , we observe that 8=7+1 . The quadratic residues of $GF(7) = \{0,1,2,3,4,5,6\}$ is the set $QR = \{0,1,2,4\}$ and the quadratic nonresidues is the set $\{3,5,6\}$. Using (3.1) , and (3.2) we construct the matrix Q and the matrix S

$$Q = \begin{pmatrix} 0 & - & - & + & - & + & + \\ + & 0 & - & - & + & - & + \\ + & + & 0 & - & - & + & - \\ - & + & + & 0 & - & - & + \\ + & - & + & + & 0 & - & - \\ - & + & - & + & + & 0 & - \\ - & - & + & - & + & + & 0 \end{pmatrix}_{7x7}, \quad S = \begin{pmatrix} 0 & -J_{1x7} \\ J_{7x1} & Q_{7x7} \end{pmatrix}_{8x8}.$$

Finally , by Theorem 4.1 , $H_8 = I_8 + S$:

$$H_8 = \begin{pmatrix} + & - & - & - & - & - & - & - \\ + & + & - & - & + & - & + & + \\ + & + & + & - & - & + & - & + \\ + & + & + & + & - & - & + & - \\ + & - & + & + & + & - & - & + \\ + & + & - & + & + & + & - & - \\ + & - & + & - & + & + & + & - \\ + & - & - & + & - & + & + & + \end{pmatrix}_{8x8} .$$

Example 4.5 : To construct a Hadamard matrix H_{12} of order 12 , there are two ways . First we observe that 12=11+1 . The quadratic residues of $GF(11)=\{\ 0,1,2,3,4,5,6,7,8,9,10\ \}$ is the set $QR=\{\ 0,1,3,4,5,9\ \}$ and the quadratic nonresidues is the set $\{\ 2,6,7,8,10\ \}$. Using (3.1) , and (3.2) , the matrices Q and S are

$$Q = \begin{pmatrix} 0 & - & + & - & - & - & + & + & + & - & + \\ + & 0 & - & + & - & - & - & + & + & + & - \\ - & + & 0 & - & + & - & - & - & + & + & + \\ + & - & + & 0 & - & + & - & - & - & + & + \\ + & + & - & + & 0 & - & + & - & - & - & + \\ + & + & + & - & + & 0 & - & + & - & - & - \\ - & + & + & + & - & + & 0 & - & + & - & - \\ - & - & + & + & + & - & + & 0 & - & + & - \\ - & - & - & + & + & + & - & + & 0 & - & + \\ + & - & - & - & + & + & + & - & + & 0 & - \\ - & + & - & - & - & + & + & + & - & + & 0 \end{pmatrix}_{11x11} ,$$

$$S = \begin{pmatrix} 0 & -J_{1x11} \\ J_{11x1} & Q_{11x11} \end{pmatrix}_{12x12} .$$

Thus , by Theorem 4.1 , $H_{12} = I_{12} + S$ is the skew Hadamard matrix displayed below:

$$H_{12} = \begin{pmatrix} + & - & - & - & - & - & - & - & - & - & - & - \\ + & + & - & + & - & - & - & + & + & + & - & + \\ + & + & + & - & + & - & - & - & + & + & + & - \\ + & - & + & + & - & + & - & - & - & + & + & + \\ + & + & - & + & + & - & + & - & - & - & + & + \\ + & + & + & - & + & + & - & + & - & - & - & + \\ + & + & + & + & - & + & + & - & + & - & - & - \\ + & - & + & + & + & - & + & + & - & + & - & - \\ + & - & - & + & + & + & - & + & + & - & + & - \\ + & - & - & - & + & + & + & - & + & + & - & + \\ + & + & - & - & - & + & + & + & - & + & + & - \\ + & - & + & - & - & - & + & + & + & - & + & + \end{pmatrix}_{12x12} .$$

Now we construct H_{12} by the second Paley construction . As 12=2(5+1) , where 5 is a prime and $5 + 1 \equiv 2 \pmod 4$, we can use Theorem 4.4 and Example 4.2 to construct H_{12}. From Example 4.2, and Theorem 4.4 (ii) ,

$$T_6 = \begin{pmatrix} 0 & + & + & + & + & + \\ + & 0 & + & - & - & + \\ + & + & 0 & + & - & - \\ + & - & + & 0 & + & - \\ + & - & - & + & 0 & + \\ + & + & - & - & + & 0 \end{pmatrix}_{6x6} , \text{ and } H_{12} = \begin{pmatrix} T_6 + I_6 & T_6 - I_6 \\ T_6 - I_6 & -(T_6 + I_6) \end{pmatrix} .$$

Hence H_{12} is the symmetric Hadamard matrix displayed below :

$$H_{12} = \begin{pmatrix} + & + & + & + & + & + & - & + & + & + & + & + \\ + & + & + & - & - & + & + & - & + & - & - & + \\ + & + & + & + & - & - & + & + & - & + & - & - \\ + & - & + & + & + & - & + & - & + & - & + & - \\ + & - & - & + & + & + & + & - & - & + & - & + \\ + & + & - & - & + & + & + & + & - & - & + & - \\ - & + & + & + & + & + & - & - & - & - & - & - \\ + & - & + & - & - & + & - & - & - & + & + & - \\ + & + & - & + & - & - & - & - & - & - & + & + \\ + & - & + & - & + & - & - & + & - & - & - & + \\ + & - & - & + & - & + & - & + & + & - & - & - \\ + & + & - & - & + & - & - & - & + & + & - & - \end{pmatrix}_{12x12}.$$

Example 4.6 : We construct a Hadamard matrix of order 20 by the Second Paley construction . As 20=2(9+1), where 9 is a power of a prime and $9+1 \equiv 2 \pmod 4$, we can use Theorem 4.4 and Example 4.3 to construct H_{20} as follows (we display T_{10} below, it is obtained from Example 4.3) :

$$T_{10} = \begin{pmatrix} 0 & + & + & + & + & + & + & + & + & + \\ + & 0 & + & - & + & - & + & - & + & - \\ + & + & 0 & - & - & - & + & + & - & + \\ + & - & - & 0 & + & + & + & - & + & - \\ + & + & - & + & 0 & - & - & - & + & + \\ + & - & - & + & - & 0 & + & + & + & - \\ + & + & + & + & - & + & 0 & - & - & - \\ + & - & + & - & - & + & - & 0 & + & + \\ + & + & - & - & + & + & - & + & 0 & - \\ + & - & + & + & + & - & - & + & - & 0 \end{pmatrix}_{10\times 10},$$

and then by Theorem 4.4 (ii)

$$H_{20} = \begin{pmatrix} T_{10}+I_{10} & T_{10}-I_{10} \\ T_{10}-I_{10} & -(T_{10}+I_{10}) \end{pmatrix}.$$

A full display of H_{20} is below :

$H_{20} =$

$$\begin{pmatrix}
+ & + & + & + & + & + & + & + & + & + & - & + & + & + & + & + & + & + & + & + \\
+ & + & + & - & + & - & + & - & + & - & + & - & + & - & + & - & + & - & + & - \\
+ & + & + & - & - & - & + & + & - & + & + & + & - & - & - & - & + & + & - & + \\
+ & - & - & + & + & + & + & - & - & + & + & - & - & - & + & + & + & - & - & + \\
+ & + & - & + & + & - & - & - & + & + & + & + & - & + & - & - & - & - & + & + \\
+ & - & - & + & - & + & + & + & + & - & + & - & - & + & - & - & + & + & + & - \\
+ & + & + & + & - & + & + & - & - & - & + & + & + & + & - & + & - & - & - & - \\
+ & - & + & - & - & + & - & + & + & + & + & - & + & - & - & + & - & - & + & + \\
+ & + & - & - & + & + & - & + & + & - & + & + & - & - & + & + & - & + & - & - \\
+ & - & + & + & + & - & - & + & - & + & + & - & + & + & + & - & - & + & - & - \\
- & + & + & + & + & + & + & + & + & + & - & - & - & - & - & - & - & - & - & - \\
+ & - & + & - & + & - & + & - & + & - & - & - & - & + & - & + & - & + & - & + \\
+ & + & - & - & - & - & + & + & - & + & - & - & - & + & + & + & - & - & + & - \\
+ & - & - & - & + & + & + & - & - & + & - & + & + & - & - & - & - & + & + & - \\
+ & + & - & + & - & - & - & - & + & + & - & - & + & - & - & + & + & + & - & - \\
+ & - & - & + & - & - & + & + & + & - & - & + & + & - & + & - & - & - & - & + \\
+ & + & + & + & - & + & - & - & - & - & - & - & - & - & + & - & - & + & + & + \\
+ & - & + & - & - & + & - & - & + & + & - & + & + & - & + & - & - & - & - & - \\
+ & + & - & - & + & + & - & + & - & - & - & + & + & - & - & + & - & - & + & \\
+ & - & + & + & + & - & - & + & - & - & - & + & - & - & - & + & + & - & + & - \\
\end{pmatrix}_{20\times 20}$$

References

[1]. Belevitch, V. 1950. Theory of 2^n - terminal networks with application to conference telephony. *Electron*. *Commun*. 27: 231-244 .

[2]. Goethals, J. M. and Seidel, J. J. 1967. Orthogonal matrices with zero diagonal. *Canad. J. Math*. 19: 1001-1010 .

[3]. Hardy, G. H., and Wright, E. M. 1954. *An introduction to the theory of numbers*. Oxford University Press, London .

[4]. Hall, M. 1967. *Combinatorial Theory*. Blaisdell (Ginn), Waltham, Mass .

[5]. Herstein, I. N. 1996. *Abstract Algebra,* third edition. Prentice-Hall Inc., New Jersey.

[6]. Leghwel A., "On Some Characterizations of Hadamard Matrices", Journal of Humanities and Applied Science, June issue no. 24 (2014), 20-41 .

[7]. Paley, R. E. A. C. 1933. On orthogonal matrices. *J. Math. and Physics*. 12: 311-320.

[8]. Ragahavarao, D. 1971. *Constructions and Combinatorial Problems in Design of Experiments*. John Wiley and Sons Inc., New York .

[9]. Wallis, W. D. and Street, Anne Penfold. 1972. *Combinatorics : Room squares, sum-free sets, Hadamard matrices*. Lecture Notes in Mathematics 292. Springer-Verlag, Berlin, Heidelberg, New York .

[10]. Williamson, J. 1944. Hadamard's determinant theorem and the sum of four squares. *Duke Math. J.* 11: 65-81 .