RATIONAL G-CIRCULANTS SATISFYING THE MATRIX EQUATION $A^2 = dI + \lambda J$

Thesis by

Clement Wing Hong Lam

In Partial Fulfillment of the Requirement
for the Degree of
Doctor of Philosophy

California Institute of Technology
Pasadena, California
1974

(Submitted March 5, 1974)

ACKNOWLEDGMENTS

I wish to express my gratitude to Professor H. J. Ryser for his invaluable assistance in the preparation of this thesis. I would also like to thank Professor O. T. Todd and Professor H. H. Kisilevsky for many helpful conversations on this and related topics. Special thanks go to the California Institute of Technology and the United States Army Research Office at Durham for their financial support in the form of a teaching and a research assistantship, respectively. Finally, I would like to thank my wife, Lily, for her encouragement and help in preparing the manuscript.

ABSTRACT

A g-circulant is a square matrix of rational numbers in which each row is obtained from the preceding row by shifting the elements cyclically g columns to the right. This work studies g-circulants A which satisfy the matrix equation $A^2 = dI + \lambda J$, where I is the identity matrix and J is the matrix of 1's. Necessary and sufficient conditions are given for the existence of solutions when $g = 1$. The existence of (0, 1) g-circulants satisfying $A^2 = dI + \lambda J$ is shown to be equivalent to the existence of (v, k, λ, g)-addition sets, which are generalizations of difference sets. It is proved that there are no non-trivial $(v, k, \lambda, 1)$-addition sets. Some examples of (v, k, λ, g)-addition sets are given and the multiplier theorem for (v, k, λ, g)-addition sets is also proved.

TABLE OF CONTENTS

Chapter 1

INTRODUCTION

A g-circulant matrix, or simply a g-circulant, is an $n \times n$ square matrix of rational numbers, in which each row (except the first) is obtained from the preceding row by shifting the elements cyclically g columns to the right.

The connection between the elements a_{ij} of the ith row and elements of the preceding row is given by

$$a_{ij} = a_{i-1, j-g} , \tag{1.1}$$

where indices are reduced to their least positive remainders modulo n.

A 1-circulant will simply be called a circulant.

A primitive g-circulant is a $(0, 1)$ - $n \times n$ matrix P_g defined as follows:

$$P_g = \left\{ \begin{array}{ll} p_{ij} = 1 & \text{if} \quad j \equiv gi \pmod{n} \\ p_{ij} = 0 & \text{otherwise} \end{array} \right\} , \tag{1.2}$$

where the indices run from 0 to $n-1$. It can be easily seen that P_g is indeed a g-circulant.

Unless otherwise specified, the indices for an $n \times n$ matrix will run from 0 to $n-1$.

The circulant with 1's in the $(0, 1)$, $(1, 2)$, $\ldots$, $(n-1, 0)$ positions and with 0's elsewhere will be denoted by C.

A generalized Hall polynomial, or simply a Hall polynomial, of a g-circulant matrix A is the polynomial

$$\theta_A(x) = \sum_{i=0}^{n-1} a_i x^i , \tag{1.3}$$

where $(a_0, a_1, \ldots, a_{n-1})$ is the first row of A.

A <u>(v, k, λ) - difference set</u> $D = \{d_1, d_2, \ldots, d_k\}$ is a collection of k residues modulo v, such that for any residue $\alpha \not\equiv 0 \pmod{v}$, the congruence

$$d_i - d_j \equiv \alpha \pmod{v} \tag{1.4}$$

has exactly λ solution pairs (d_i, d_j) with d_i and d_j in D.

With every (v, k, λ) - difference set D, we associate a matrix A given by

$$A = \sum_{i=1}^{k} C^{d_i} . \tag{1.5}$$

This is called the incidence matrix of the (v, k, λ) - difference set. When the meaning is clear from the context, the incidence matrix will be called a difference set.

The matrix J will denote the matrix with all 1's. The matrix I will be the identity matrix.

G-circulants have appeared in many recent combinatorial problems. Knuth [1970] investigated the (0, 1) - matrices A which satisfy the relation

$$A^2 = J . \tag{1.6}$$

A necessary condition for a solution is that the order n of the matrix is a square. Indeed, when n is a square, there exists a $\sqrt{n}$-circulant which satisfies (1.6).

Ryser [1970] investigated (0, 1) - matrices A of order n which satisfy the matrix equation $A^2=D+\lambda J$, where D is a diagonal matrix. He showed that apart from certain exceptional matrices, A must satisfy

$$A^2 = dI + \lambda J , \tag{1.7}$$

where in (1.7) the matrix A has constant line sums c, and the parameters satisfy the conditions

$$c^2 = d + \lambda n \tag{1.8}$$

and

$$-\lambda < d \leq c - \lambda . \tag{1.9}$$

Again for $d = 1$, and any parameter set that satisfies (1.8) and (1.9), a c-circulant exists, satisfying (1.7).

A g-circulant matrix can also be considered as an adjacency matrix of a graph. Such graphs have been given many names: cyclic graphs, starred polygons, etc. (Elspas and Turner [1970], Turner [1967], Tuero [1961], and Berggren [1962]).

Albow and Brenner [1963] have derived some elementary multiplicative properties of g-circulants, which will be summarized in Chapter 2. However, the main purpose of this work is to investigate the existence of rational g-circulants which satisfy the matrix equation (1.7).

It should be pointed out that the eigenvalues of a g-circulant are especially easy to calculate. (Albow and Brenner [1963]). Equation (1.7) puts a severe restriction on the possible eigenvalues of A. This "eigenvalue" approach has been successful in the study of many combinatorial problems: Ryser [1970], Hoffman and Singleton [1960]. However, in the study of g-circulants, the theory of polynomial congruences is a more suitable and powerful technique. First of all, it implies the same conditions on the eigenvalues. But, more importantly, the Chinese remainder theorem is a powerful tool in constructing solutions. With this remark, we proceed with the study of g-circulants.

Chapter 2

ELEMENTARY PROPERTIES OF G-CIRCULANTS

The first two theorems are taken from Albow and Brenner [1963]. They are elementary and are quoted without proof.

Theorem 2.1 (Albow and Brenner) The equation

$$CA = AC^g \tag{2.1}$$

characterizes the g-circulant property of A. That is, the matrix A is a g-circulant if and only if relation (2.1) is valid.

Corollary 2.2 $CP_g = P_g C^g$.

Proof: Since P_g is a g-circulant, Corollary 2.2 follows from Theorem 2.1.

Theorem 2.3 (Albow and Brenner) If A is a g-circulant and B is an h-circulant, then AB is a gh-circulant.

Corollary 2.4 $P_g P_h = P_{gh} = P_h P_g$.

Proof: By Theorem 2.3, $P_g P_h$ is a gh-circulant. Moreover, its first row is identical to that of P_{gh}. Thus $P_g P_h = P_{gh}$. Similarly for $P_h P_g = P_{gh}$.

Corollary 2.5 If A is a g-circulant, with $(a_0, a_1, \ldots, a_{n-1})$ as its first row, then

$$A = P_g \left(\sum_{i=0}^{n-1} a_i C^i \right). \tag{2.2}$$

Proof: It is easy to see that the first row of the right hand side of relation (2.2) is $(a_0, a_1, \ldots, a_{n-1})$. Moreover, if we multiply the right hand side of (2.2) by C on the left, we get

$$CP_g\left(\sum_{i=0}^{n-1} a_i C^i\right) = P_g C^g\left(\sum_{i=0}^{n-1} a_i C^i\right)$$
$$= P_g\left(\sum_{i=0}^{n-1} a_i C^i\right)C^g .$$

Thus, the right hand side of (2.2) is a g-circulant. So, relation (2.2) holds.

Conversely, we note that a matrix of the form (2.2) is a g-circulant because it is the product of a g-circulant and a 1-circulant.

Theorem 2.6 If A is a g-circulant and if B is an h-circulant with $\theta_A(x)$ and $\theta_B(x)$ as their respective generalized Hall polynomials, then the generalized Hall polynomial of AB is given by

$$\theta_{AB}(x) = \theta_A(x^h)\,\theta_B(x) \pmod{x^n-1}. \qquad (2.3)$$

Proof: Let $(a_0, a_1, \ldots, a_{n-1})$ and $(b_0, b_1, \ldots, b_{n-1})$ be the first rows of A and B, respectively. The generalized Hall polynomials of A and B are

$$\theta_A(x) = \sum_{i=0}^{n-1} a_i x^i ,$$

and

$$\theta_B(x) = \sum_{i=0}^{n-1} b_i x^i ,$$

respectively.

By Corollary 2.5,

$$A = P_g \sum_{i=0}^{n-1} a_i C^i \quad ,$$

and

$$B = P_h \sum_{i=0}^{n-1} b_i C^i \quad .$$

Hence,

$$\begin{aligned} AB &= P_g\left(\sum_{i=0}^{n-1} a_i C^i\right) \cdot P_h\left(\sum_{i=0}^{n-1} b_i C^i\right) \\ &= P_g P_h\left(\sum_{i=0}^{n-1} a_i C^{hi}\right)\left(\sum_{i=0}^{n-1} b_i C^i\right) \\ &= P_{gh}\left(\sum_{i=0}^{n-1} a_i C^{hi}\right)\left(\sum_{i=0}^{n-1} b_i C^i\right) \quad . \end{aligned}$$

Since circulants multiply like polynomials (mod x^n-1) and $\theta_{AB}(x)$ is defined by $\left(\sum_{i=0}^{n-1} a_i C^{hi}\right)\left(\sum_{i=0}^{n-1} b_i C^i\right)$, we have

$$\theta_{AB}(x) = \theta_A(x^h)\, \theta_B(x) \pmod{x^n-1} \, .$$

Chapter 3

RATIONAL G-CIRCULANTS SATISFYING $A^2 = dI + \lambda J$

In this chapter, we will be considering g-circulants which satisfy the matrix equation

$$A^2 = dI + \lambda J \ , \tag{3.1}$$

where d and λ are rational numbers. By applying Corollary 2.4 and Theorem 2.6 to this special case, we obtain the following result.

Theorem 3.1 Let d and λ be rational numbers. An $n \times n$ g-circulant A satisfies (3.1) if, and only if

$$\begin{aligned} &\text{(i)} \quad d \neq 0 \text{ implies } g^2 \equiv 1 \pmod{n} , \\ &\text{(ii)} \quad \theta_A(x^g)\, \theta_A(x) \equiv d + \lambda\, T(x) \pmod{x^n - 1} \ , \end{aligned} \tag{3.2}$$

where $$T(x) = 1 + x + \ldots x^{n-1} \ .$$

Proof: If A satisfies (3.1), then (ii) follows from Theorem 2.6. Moreover, if $d \neq 0$, then $dI + \lambda J$ is a 1-circulant, and Theorem 2.3 implies that $g^2 \equiv 1 \pmod{n}$. If a g-circulant A satisfies (3.2), (ii) implies that the first row of A^2 is equal to the first row of $dI + \lambda J$. Now, if $d = 0$, (ii) is enough to assure that $A^2 = \lambda J$. If $d \neq 0$, (i) implies that A^2 is a 1-circulant, and we have $A^2 = dI + \lambda J$.

Next, we want to look carefully at the polynomial congruence relation

$$\theta_A(x^g)\, \theta_A(x) \equiv d + \lambda T(x) \pmod{x^n - 1} \ . \tag{3.3}$$

In the remaining parts of this work, we are only concerned with the matrix equation $A^2 = dI + \lambda J$, and in this context, there is no ambiguity in writing $\theta(x)$ for $\theta_A(x\ )$.

Let $\varphi_\omega(x)$ be the monic polynomial satisfied by the primitive ω-th root of unity over the rational field, i.e. the <u>ω-th cyclotomic polynomial.</u> It is well known that this polynomial is irreducible over the rationals, and that $Q[x]/\varphi_\omega(x)$ is isomorphic to the cyclotomic field $Q(\xi_\omega)$, where $Q[x]$ is the polynomial ring with rational coefficients, ξ_ω is a primitive ω-th root of unity, and Q is the field of rational numbers.

Let us look at equation (3. 3) modulo the various $\varphi_\omega(x)$'s, where ω divides n. These reduced polynomial congruence relations are easier to solve, and we will construct a solution to (3. 3) using the Chinese remainder theorem.

We let the remainder of $\theta(x)$ taken modulo $\varphi_\omega(x)$ be $\theta_\omega(x)$. As $\varphi_\omega(x)$ divides $\varphi_\omega(x^g)$ when $(g, \omega) = 1$, we find that the remainder of $\theta(x^g)$ taken modulo $\varphi_\omega(x)$ is $\theta_\omega(x^g)$. Since ω divides n, $\varphi_\omega(x)$ divides x^n-1. Relation (3. 3), when taken modulo $\varphi_\omega(x)$, gives

$$\theta_\omega(x^g)\theta_\omega(x) \equiv d + \lambda T(x) \pmod{\varphi_\omega(x)}. \tag{3. 4}$$

For $\omega = 1$, $\varphi_\omega(x) = x - 1$, and $Q[x]/(x-1)$ is merely Q. Now, (3. 4) becomes a numerical relationship,

$$\theta(1^g)\theta(1) = d + \lambda T(1)$$

or

$$c^2 = d + \lambda n\ ,$$

where $c = \theta(1^g)$ is the row sum of the g-circulant A.

For $\omega \neq 1$, $\varphi_\omega(x)$ divides $T(x)$. Thus (3.4) becomes

$$\theta_\omega(x^g)\,\theta_\omega(x) \equiv d \pmod{\varphi_\omega(x)} \ . \tag{3.5}$$

It follows that (3.5) induces a factorization of d in $Q(\xi_\omega)$, namely

$$\theta_\omega(\xi_\omega^g)\,\theta_\omega(\xi_\omega) = d \ , \tag{3.6}$$

and vice versa. This is because the isomorphism between $Q[x]/\varphi_\omega(x)$ and $Q(\xi_\omega)$ can be obtained by mapping $f(x)$ of $Q[x]/\varphi_\omega(x)$ onto $f(\xi_\omega)$ in $Q(\xi_\omega)$. Results in difference sets corresponding to (3.5) and (3.6) have been noted in Baumert [1971].

The Chinese remainder theorem establishes the isomorphism

$$Q[x]/x^n\text{-}1 \cong \prod_{\omega | n} \left(Q[x]/\varphi_\omega(x)\right) . \tag{3.7}$$

Thus, if we are given a set of polynomials $\theta_\omega(x)$'s corresponding to the various $\varphi_\omega(x)$'s, we can find a unique $\theta(x)$ modulo $x^n\text{-}1$, such that for all $\omega | n$,

$$\theta(x) \equiv \theta_\omega(x) \pmod{\varphi_\omega(x)} \ .$$

In fact, Baumert gives an explicit formula for determining $\theta(x)$. Thus

$$\theta(x) \equiv \frac{1}{n} \sum_{\omega | n} \theta_\omega(x)\, B_{n,\,\omega}(x) \pmod{x^n\text{-}1} , \tag{3.8}$$

where

$$B_{n,\,\omega}(x) = \sum_{r | \omega} \mu(\tfrac{\omega}{r})\, r\, \frac{x^n\text{-}1}{x^r\text{-}1} \ , \tag{3.9}$$

and μ is the Möbius function.

With the above observations, we can prove the following theorem.

Theorem 3.2 Let d and λ be rational numbers. An $n \times n$ g-circulant A satisfies the matrix equation

$$A^2 = dI + \lambda J$$

if and only if

(i) $d \neq 0$ implies $g^2 \equiv 1 \pmod{n}$ (3.10)

(ii) the row sum c of A satisfies

$$c^2 = d + \lambda n \tag{3.11}$$

and

(iii) for all divisors ω of n, $\omega \neq 1$,

$$\theta_\omega(\xi_\omega^g)\, \theta_\omega(\xi_\omega) = d \ , \tag{3.12}$$

where ξ_ω is a primitive ω-th root of unity, and $\theta_\omega(x)$ is the remainder of the Hall polynomial of A taken modulo $\varphi_\omega(x)$.

Proof: Assume that a g-circulant A satisfies the matrix equation $A^2 = dI + \lambda J$. Condition (i) of Theorem 3.1 implies (3.10). Condition (ii) of the same theorem implies that the Hall polynomial of A satisfies

$$\theta(x^g)\, \theta(x) \equiv d + \lambda T(x) \pmod{x^n - 1} \ . \tag{3.13}$$

Let ω be a divisor of n and $\varphi_\omega(x)$ the ω-th cyclotomic polynomial. Relation (3.13), when taken modulo $\varphi_\omega(x)$ becomes

$$\theta_\omega(x^g)\, \theta_\omega(x) \equiv d + \lambda T(x) \pmod{\varphi_\omega(x)} \ , \tag{3.14}$$

where $\theta_\omega(x)$ is the remainder of $\theta(x)$ taken modulo $\varphi_\omega(x)$.

For $\omega = 1$, (3.14) gives the relationship (3.11).

For $\omega \neq 1$, (3.14) becomes

$$\theta_\omega(x^g)\ \theta_\omega(x) \equiv d \quad (\mathrm{mod}\ \varphi_\omega(x)) \ . \tag{3.15}$$

It follows that (3.15) induces a factorization of d in $Q(\xi_\omega)$ of the form (3.12), and we have proved the necessary part of the theorem.

Next, we assume that A is a g - circulant with $\theta(x)$ as its Hall polynomial. Because of the isomorphism between $Q[x]/\varphi_\omega(x)$ and $Q(\xi_\omega)$, (3.12) induces the polynomial congruence

$$\theta_\omega(x^g)\ \theta_\omega(x) \equiv d \quad (\mathrm{mod}\ \varphi_\omega(x)) \ , \tag{3.16}$$

for all divisors ω of n not equal to 1. When $\omega = 1$, $\varphi_1(x) = (x-1)$ and (3.11) implies that

$$\theta_1(x^g)\ \theta_1(x) \equiv d + \lambda n \quad (\mathrm{mod}\ \varphi_1(x)) \ . \tag{3.17}$$

Since $\theta_\omega(x)$ is merely the remainder of the Hall polynomial of A taken modulo $\varphi_\omega(x)$, relation (3.17) can be written as

$$\theta(x^g)\ \theta(x) \equiv d + \lambda n \quad (\mathrm{mod}\ \varphi_1(x)) \ . \tag{3.18}$$

And (3.16) can be written as

$$\theta(x^g)\ \theta(x) \equiv d \quad (\mathrm{mod}\ \varphi_\omega(x)) \ , \tag{3.19}$$

for all divisors ω of n not equal to 1.

Hence we find that $\theta(x^g)\ \theta(x)$ satisfies all of the congruences in (3.18) and (3.19). Since $d + \lambda T(x)$ is also congruent to d modulo $\varphi_\omega(x)$

for $\omega \neq 1$ and congruent to $d + \lambda n$ modulo $\varphi_1(x)$, the Chinese remainder theorem implies that

$$\theta(x^g)\,\theta(x) \equiv d + \lambda T(x) \pmod{x^n - 1} .$$

Now, together with (3.10), the conditions (i) and (ii) of Theorem 3.1 are satisfied, and hence A satisfies the matrix equation $A^2 = dI + \lambda J$.

In fact, Theorem 3.2 gives us a method of constructing solutions for (3.1) when the conditions of Theorem 3.2 are satisfied. However, we have to interpret (3.12) carefully.

In the field $Q(\xi_\omega)$, every element can be represented as

$$\sum_{i=0}^{\Phi(\omega)-1} a_i \xi_\omega^i, \qquad \text{where} \qquad a_i \in Q, \quad \text{and}$$

$\Phi(\omega)$ is the Euler Φ-function.

If $g^2 \equiv 1 \pmod{n}$, $(g, \omega) = 1$ for all divisors ω of n. The map σ sending ξ_ω to ξ_ω^g is an automorphism of Q. Now (3.12) can be interpreted as saying that d factorizes in $Q(\xi_\omega)$ into a product of $\theta_\omega(\xi_\omega)$ and its image $\theta_\omega(\xi_\omega^g)$ under the map σ.

We now prove the following theorem.

Theorem 3.3 Let d and λ be rational numbers, and $g^2 \equiv 1 \pmod{n}$. Suppose we have

(i) $d + \lambda n$ is a rational square, and (3.20)

(ii) for every $\omega | n$ not equal to 1, d factors in $Q(\xi_\omega)$ as

$$\theta_\omega(\xi_\omega^g)\,\theta_\omega(\xi_\omega) = d. , \tag{3.21}$$

for some $\theta_\omega(\xi_\omega)$ in $Q(\xi_\omega)$.

Then there exists an $n \times n$ g-circulant A which satisfies (3.1).

Proof: Using the isomorphism between $Q(\xi_\omega)$ and $Q[x]/\varphi_\omega(x)$, for each ω, we can define a polynomial $\theta_\omega(x)$ such that

$$\theta_\omega(x^g)\ \theta_\omega(x) \equiv d \pmod{\varphi_\omega(x)}. \tag{3.22}$$

Using the Chinese remainder theorem, we can define a polynomial $\theta(x)$ in $Q[x]/x^n-1$, such that

$$\theta(x) \equiv \theta_\omega(x) \pmod{\varphi_\omega(x)} \tag{3.23}$$

for all $\omega|n$ not equal to 1, and

$$\theta(x) \equiv \sqrt{d+\lambda n} \pmod{\varphi_1(x)}. \tag{3.24}$$

Putting x^g for x in (3.23), we obtain

$$\theta(x^g) \equiv \theta_\omega(x^g) \pmod{\varphi_\omega(x^g)}. \tag{3.25}$$

But $(g, \omega) = 1$ as $g^2 \equiv 1 \pmod{n}$; hence $\varphi_\omega(x)$ divides $\varphi_\omega(x^g)$. Hence (3.24) implies

$$\theta(x^g) \equiv \theta_\omega(x^g) \pmod{\varphi_\omega(x)}. \tag{3.26}$$

We now define an $n \times n$ g-circulant A with $\theta(x)$ as its Hall polynomial. Then $\theta_\omega(x)$ will be the remainder of the Hall polynomial of A taken modulo $\varphi_\omega(x)$. The conditions of Theorem 3.2 are satisfied and hence A satisfies (3.1).

The problem of finding g-circulant solutions to (3. 1) now reduces to the problem of determining when d can be factorized into the special form of (3. 21). The problem involving general g's is very complicated. However, for $g = 1$, (3. 21) is equivalent to the requirement that the polynomial $x^2 - d$ has both of its roots in $Q(\xi_\omega)$, and in this case we say that d is a square in $Q(\xi_\omega)$. The next chapter carries this investigation further.

Chapter 4

THE CASE $g = 1$

In this chapter we will solve the equation

$$A^2 = dI + \lambda J , \tag{4.1}$$

where the matrix A is a rational circulant. Since $g = 1$ we automatically have $g^2 \equiv 1 (\text{mod } n)$. Moreover, in condition (3.21), $\theta_\omega(\xi_\omega^g)$ is now simply $\theta_\omega(\xi_\omega)$. Thus, the conditions in Theorem 3.3 are simplified to

(i) $d + \lambda n$ is a rational square, and (4.2)

(ii) d is a square in every cyclotomic field $Q(\xi_\omega)$, where ω is a divisor of n and not equal to 1. (4.3)

If d is itself a rational square, condition (4.3) is automatically satisfied. The study of the case where d is not a rational square requires the following number theoretical lemma. Many of the facts quoted can be found in Lang [1965].

<u>Lemma 4.1</u> Let p be an odd prime and let ξ_{p^k} be a p^k-th root of unity, where $k \geq 1$. Then the cyclotomic field $Q(\xi_{p^k})$ has a unique quadratic subfield $Q\left(\sqrt{(-1)^{(p-1)/2}\, p}\right)$.

Proof: When p is an odd prime, the Galois group of the cyclotomic field $Q(\xi_{p^k})$ over Q is cyclic; in fact, it is isomorphic to the multiplicative group $(\mathbb{Z}/p^k\mathbb{Z})^*$ of residues modulo p^k that are relatively prime to p. The degree of the field extension is $\Phi(p^k)$, where $\Phi(x)$ is the Euler Φ-function. It is well known that

$$\Phi(p^k) = (p-1)p^{k-1}.$$

Since p is an odd prime, $\Phi(p^k)$ is even. Thus, there exists a unique subgroup of index 2 in the Galois group, and correspondingly a unique quadratic subfield. It is well known that the quadratic subfield in $Q(\xi_p)$ is $Q\left(\sqrt{(-1)^{(p-1)/2}p}\right)$. As $Q(\xi_p)$ is a subfield in $Q(\xi_{p^k})$, this is the unique quadratic subfield.

The next theorem gives the necessary and sufficient condition for the existence of a solution to (4.1). Moreover, it gives the number of distinct solutions. Here two solutions are treated as distinct provided their Hall polynomials are different.

We will use the Legendre symbol $\left(\frac{-1}{p}\right)$ for $(-1)^{\frac{p-1}{2}}$, and $\tau(n)$ will denote the number of divisors of n.

<u>Theorem 4.2</u> Let A be a rational circulant matrix of order $n > 1$. The matrix equation

$$A^2 = dI + \lambda J \tag{4.4}$$

has a solution if and only if

d + λn is a rational square, and (4.5)

d is a ration square unless n is a power of an odd prime p, in which case it can also be the product of a rational square with $\left(\frac{-1}{p}\right)p$. (4.6)

Moreover, if a solution exists, the number of distinct solutions is found as follows:

if $d = 0$ and $\lambda = 0$, then there is only one solution, $A = 0$; (4.7)

if $d = 0$ and $\lambda \neq 0$, then there are two solutions; (4.8) if $d \neq 0$ and $d + \lambda n = 0$, then there are $2^{\tau(n)-1}$ solutions; and (4.9)

if $d \neq 0$ and $d + \lambda n \neq 0$, then there are $2^{\tau(n)}$ solutions. (4.10)

Proof: Assume that both conditions (4.5) and (4.6) are satisfied. Condition (4.5) is the same as condition (4.2). If d is a square, then condition (4.3) is also satisfied. If d is not a rational square, condition (4.6) implies that n is a power of an odd prime, and that d is the product of a rational square with $\left(\frac{-1}{p}\right)p$. In this case, we can show that d is still a square in all the cyclotomic fields of condition (4.3). This is because all the divisors of n are powers of the same odd prime. Hence, Lemma 4.1 implies that all of these fields have the same quadratic subfield $Q\left(\sqrt{\left(\frac{-1}{p}\right)p}\right)$. The fact that d is a square in this quadratic subfield implies that it is a square in all the cyclotomic fields in question. Hence, conditions (4.5) and (4.6) are equivalent to the conditions (4.2) and (4.3). Using the Chinese remainder theorem, we can construct a $\theta(x)$ such that

$$[\theta(x)]^2 \equiv d + \lambda T(x) \pmod{x^n - 1}\,. \tag{4.11}$$

The existence of $\theta(x)$ satisfying (4.11) is equivalent to the existence of a rational circulant satisfying the matrix equation (4.4), and we have proved the sufficient part of the theorem.

Next, we suppose that there exists a solution of (4.4). Then (4.5) must be satisfied. To prove (4.6), we have to prove that if d is not a rational square, then n is a power of an odd prime p and d is a product of a rational square with $\left(\frac{-1}{p}\right)p$.

If n is even, then by (4.3), d is a square in $Q(\xi_2)$. But

$\xi_2 = -1$ and $Q(\xi_2) = Q$. Thus (4.3) implies that d is a square in Q, contradicting the assumption that d is not a rational square.

Let p be an odd prime dividing n. Then (4.3) implies that d is a square in $Q(\xi_p)$, that is $d = \alpha^2$, α not in Q. But then $Q(\alpha)$ is a quadratic subfield of $Q(\xi_p)$. By Lemma 4.1, the quadratic subfield is unique. Hence

$$\alpha = a + b \cdot \sqrt{\left(\frac{-1}{p}\right)p} \quad \text{for some a, b in Q.}$$

Hence

$$\alpha^2 = a^2 + \left(\frac{-1}{p}\right)b^2 p + 2ab \cdot \sqrt{\left(\frac{-1}{p}\right)p} \ . \tag{4.12}$$

Since $d = \alpha^2$ is in Q, we have $2ab = 0$. If $b = 0$, then $\alpha = a$ and d would be a rational square. Hence $a = 0$ and

$$d = \left(\frac{-1}{p}\right)b^2 p \, , \tag{4.13}$$

which is the required form.

Suppose there exists another odd prime $q \neq p$ which divides n. By similar reasoning

$$d = \left(\frac{-1}{q}\right)c^2 q, \quad \text{where } c \in Q. \tag{4.14}$$

But (4.13) and (4.14) together imply that either p/q or $-p/q$ is a rational square, and this is impossible. Hence n must be the power of an odd prime.

It still remains for us to count the number of distinct solutions. In constructing solutions, we use the Chinese remainder theorem to construct a polynomial $\theta(x)$ in $Q[x]/x^n-1$ such that

$$\theta(x)^2 \equiv d + \lambda n \quad (\text{mod } x-1) \tag{4.15}$$

and $$\theta(x)^2 \equiv d \qquad \left(\bmod \varphi_\omega(x)\right), \tag{4.16}$$

where ω divides n and is not equal to 1. Hence $\theta(x)$ is congruent to the square roots of the right hand sides of (4.15) and (4.16). In taking square roots, different choice of sign will give us different $\theta(x)$'s, as long as the terms involved are not equal to 0. So, we have to look at the cases involving 0's separately. When both d and $d+\lambda n$ are non-zero, there are a total of $\tau(n)$ square roots. Hence there are $2^{\tau(n)}$ solutions in this case.

If $d = 0$ and $\lambda = 0$, the equation reduces to $A^2 = 0$. If $\theta(x)$ is the Hall polynomial of A,

$$\theta(x) \equiv 0 \qquad \left(\bmod \varphi_\omega(x)\right)$$

for all divisors ω of n. The only possible solution is for $\theta(x) = 0$. Hence there is only one solution, namely $A = 0$.

If $d = 0$ and $\lambda \neq 0$, there are two choices for the square root of λn. The other square roots in condition (4.3) are all 0's. Thus, there are only two solutions.

If $d \neq 0$ and $d + \lambda n = 0$, there are $\tau(n) - 1$ cyclotomic fields in condition (4.3), each of which gives two choices for the square root of d. Thus, there are a total of $2^{\tau(n)-1}$ choices.

Let us now look at some examples of the construction of solutions. Recall that

$$\theta(x) = \frac{1}{n} \sum_{\omega | n} \theta_\omega(x)\, B_{n,\omega}(x) \tag{4.17}$$

and

$$B_{n,\omega}(x) = \sum_{r|\omega} \mu(\tfrac{\omega}{r})\, r \left(\frac{x^n-1}{x^r-1}\right). \tag{4.18}$$

For $n = 5$, $B_{5,1}(x) = x^4 + x^3 + x^2 + x + 1$, and

$$B_{5,5}(x) = -x^4 - x^3 - x^2 - x + 4 .$$

Example 1: $d = 1$, $c = 4$ and $\lambda = 3$.

Conditions (4.2) and (4.3) give

$$\theta_1(x) = \pm 4, \quad \text{and}$$

$$\theta_5(x) = \pm 1 .$$

Consider the case $\theta_1(x) = +4$ and $\theta_5(x) = +1$.

Using (4.17),

$$\theta(x) = \frac{1}{5}(3x^4 + 3x^3 + 3x^2 + 3x + 8)$$

which satisfies $\theta(x)^2 \equiv 1 + 3T(x) \pmod{x^5-1}$.

The other 3 solutions are $x^4 + x^3 + x^2 + x$, $-\frac{1}{5}(3x^4 + 3x^3 + 3x^2 + 3x + 8)$, and $-(x^4 + x^3 + x^2 + x)$.

Example 2: $d = 5$, $c = 15$ and $\lambda = 44$.

Observe that $(\xi^4 - \xi^3 - \xi^2 + \xi)^2 = 5$ where ξ is a primitive 5th root of unity. Thus

$$\theta_1(x) = \pm 15, \quad \text{and}$$

$$\theta_5(x) = \pm(x^4 - x^3 - x^2 + x).$$

Taking the positive sign in both cases, (4.15) gives

$$\theta(x) = 4x^4 + 2x^3 + 2x^2 + 4x + 3.$$

Again, $\theta(x)$ satisfies $\theta(x)^2 \equiv 5 + 44T(x) \pmod{x^5 - 1}$.

Once we obtain a rational circulant satisfying equation (4.1), it is not difficult to get a non-negative integral circulant satisfying the equation, although possibly with a different d and λ. Suppose that A is a rational circulant satisfying (4.1). We can construct an integral circulant by multiplying A by an appropriate factor. Then we can add enough multiples of J to obtain a non-negative integral circulant. The resulting circulant still satisfies equation (4.1) except possibly with a different d and λ.

The interesting case occurs when A is a (0, 1) circulant. In the next chapter, we will classify all the (0, 1) circulant solutions to equation (4.1).

Chapter 5

ADDITION SETS

In chapter 4, we answered the question of the existence of rational 1-circulants A satisfying the matrix equation

$$A^2 = dI + \lambda J. \tag{5.1}$$

In this chapter we restrict our attention to (0, 1) 1-circulants.

There are some easy solutions to (5.1):

$$I^2 = I, \tag{5.2}$$

$$J^2 = nJ, \tag{5.3}$$

$$(J-I)^2 = I + (n-2)J, \tag{5.4}$$

and if n is even,

$$\left[C^{n/2}\right] = I, \tag{5.5}$$

$$\left[C^{n/2}(J-1)\right]^2 = I + (n-2)J, \tag{5.6}$$

where C is the special 1-circulant defined in Chapter 1.

The question now is whether there exist any other (0, 1)-circulants which satisfy (5.1). It turns out that in the (0, 1) case, the existence of such a circulant is equivalent to the existence of a mathematical object which is defined as follows.

A <u>(v, k, λ)-addition set</u> $A = \{a_1, a_2, \ldots, a_k\}$, or simply an <u>addition set</u>, is a collection of k distinct residues modulo v, such that for any residue $\alpha \not\equiv 0$ modulo v, the congruence

$$a_i + a_j \equiv \alpha \pmod{v} \tag{5.7}$$

has exactly λ solution pairs (a_i, a_j) with a_i and a_j in A.

To avoid degenerate configurations, we further require that

$$k \geq 1 \tag{5.8}$$

Remark 5.1 It can be easily seen that every addition set corresponds to a (0, 1) circulant satisfying $A^2 = dI + \lambda J$. Given an addition set A, we can define a $v \times v$ circulant A whose first row has 1's in every a_i-th position, where a_i belongs to the addition set A. The matrix A will have line sums k and will satisfy (5.1) with an appropriate d, but the same λ. Conversely, given a (0, 1) circulant A satisfying (5.1), an addition set can be formed from the first row of A.

With the above remark, there is no ambiguity in defining a Hall polynomial $\theta(x)$ for an addition set A by

$$\theta(x) = \sum_{i=1}^{k} x^{a_i}, \quad a_i \in A. \tag{5.9}$$

Observe that

$$[\theta(x)]^2 = \sum_{i,j}^{k} x^{a_i+a_j} \equiv d + \lambda T(x) \pmod{x^v-1}, \tag{5.10}$$

where $T(x) = 1 + x + x^2 + x^3 + \dots x^{v-1}$.

Here, because of the similarity of addition sets with difference sets and block designs, we change the notation for the parameters (n, c, λ) to (v, k, λ).

Corresponding to the solutions (5.2) to (5.6), we have the following addition sets

$$\begin{array}{ll} \text{(i)} & A = \{0\}\,, \\ \text{(ii)} & A = \{0,\ 1,\ \ldots,\ v-1\}\,, \\ \text{(iii)} & A = \{1,\ 2,\ \ldots,\ v-1\}\,, \\ \text{(iv)} & \text{if } v \text{ is even, } A = \{v/2\}\,, \\ \text{(v)} & \text{if } v \text{ is even, } A = \{0,\ 1,\ \ldots,\ \frac{v}{2}-1,\ \frac{v}{2}+1,\ \frac{v}{2}+2,\ \ldots,\ v-1\}. \end{array} \tag{5.11}$$

The question now is whether there are any other addition sets. The *main purpose of this chapter is to derive* Theorem 5.16 *which asserts that* (5.11) *contains all of the addition sets.*

Let us first restate the various parameter relations. We have

$$1 \le k^2 = d + \lambda v\,, \tag{5.12}$$

and

$$-\lambda < d \le k - \lambda\,. \tag{5.13}$$

Let us state some definitions which are helpful in the development of this chapter.

Let $A = \{a_1,\ a_2,\ \ldots, a_k\}$ and $B = \{a_1,\ a_2,\ \ldots, a_k\}$ be two sets of residues modulo v. An *addition table* of A and B, denoted by $A \oplus B$, is a $k \times k$ matrix, whose (i, j)-th entry is $(a_i + b_j)$ taken modulo v.

A *shift of* A *by* s, denoted by $s + A$, is

$$s + A = \{s + a_i \mid a_i \in A\}\,. \tag{5.14}$$

Similarly, a matrix $M = (m_{ij})$ is a *shift* of a matrix $N = (n_{ij})$ if there exists an integer a such that for all i, j

$$m_{ij} \equiv a + n_{ij} \pmod v\,.$$

Let 2^r divide v (r need not be maximal). A basic r-set is a set A of 2^r residues modulo v defined by

$$A = \left\{ i \frac{v}{2^r} \;\middle|\; i = 0, 1, \ldots, 2^r - 1 \right\}.$$

The addition table $A \oplus A$ is the basic r-block.

Proposition 5.2 The basic r-set A is closed under addition modulo v and each $a \in A$ appears exactly 2^r times in the basic r-block.

Proof: It is easy to see that A is closed under addition modulo v and that the entries in each row of its addition table are distinct. Hence every $a \in A$ appears in each row of the basic r-block exactly once. Thus, each $a \in A$ appears exactly 2^r times in the addition table.

Corollary 5.3 Let A be the basic r-set and let $B = b + A$ and $C = c + A$ be shifts of A by b and c, respectively. Then every residue that appears in the addition table $B \oplus C$ is from the set $(b + c) + A$, and each residue appears exactly 2^r times in $B \oplus C$.

Proof: Let M be $B \oplus C$. If we preserve the same ordering in B and C as in A, M will be just a shift of the basic r-block by $(b + c)$. Hence, all the residues that appear in M are from $(b + c) + A$ and each appears exactly 2^r times in M.

It should be remarked that if A is any set of residues, the addition table $A \oplus A$ is symmetric. If A is an addition set, then every non-zero residue occurs λ times in the addition table, and 0 occurs $(d + \lambda)$ times.

We will call any addition set that is not covered by those listed in (5.11) a new solution.

Theorem 5.4 If λ is odd, there is no new solution.

Proof: Let A be an addition set, with λ being odd, and let us consider its addition table. Since the table is symmetric, every non-zero residue α that appears in an off diagonal position (i, j) also appears in the off diagonal position (j, i). Since λ is odd, α must appear on the main diagonal an odd number of times. But there are $v-1$ non-zero α's and k diagonal positions. Hence $k \geq v-1$. But $k \leq v$. Hence $k = v$ or $v-1$. In both of these cases, the only solutions are the ones in (5.11).

Theorem 5.5 Let A be a new solution. Then v is even. Moreover, if $a \in A$ and a is not equal to 0 or $v/2$, then $a + v/2 \in A$.

Proof: If there does not exist an $a \in A$ not equal to 0 or $v/2$, then $A = \{0\}$, $\{v/2\}$, or $\{0, v/2\}$. The only addition sets in these cases are given by (5.11).

Assume then that we can choose an $a \in A$ not equal to 0 or $v/2$. Then 2a will be a non-zero entry in the main diagonal of the addition table for A. Since A is a new solution, Theorem 5.4 implies that λ is even. Hence, the non-zero residues that appear in the main diagonal must appear there an even number of times. In particular, there exists $b \in A$ not equal to a such that

$$2a \equiv 2b \pmod{v},$$

or

$$2(a-b) \equiv 0 \pmod{v}. \tag{5.15}$$

If v is odd, (5.15) implies that $a = b$, which contradicts the choice of b. Hence v is even, and the only b not equal to a which satisfies (5.15) is $b = a + v/2$.

Lemma 5.6 If $r \geq 1$, $2^r | v$ and the addition set A is a union of distinct shifts of the basic r-set, then either

(i) $k = v$, or

(ii) $2^{r+1} | v$ and the set A is a union of distinct shifts of the basic (r+1)-set.

Proof: We can rearrange A to group the shifts together, i.e. the first 2^r elements of A will be the set $d_1 + B$, where B is the basic r-set, the second 2^r elements will be $d_{2^r+1} + B$, and so on.

Since A is a union of distinct shifts, we have

$$2^r | k .$$

Let
$$s = k/_{2}r . \tag{5.16}$$

With the above rearrangement, the addition table for A will be an $s \times s$ matrix of $2^r \times 2^r$ blocks. Each of these blocks will be a shift of the basic r-block. Since every entry in a block appears 2^r times, we have

$$2^r | \lambda . \tag{5.17}$$

However, the $s \times s$ matrix of blocks is still a symmetric matrix. The off diagonal blocks again appear in pairs, one on each side of the diagonal. An entry in the off diagonal block would then appear in multiples of 2^{r+1}. If $\lambda \equiv 2^r (\text{mod } 2^{r+1})$, every non-zero residue must appear in some diagonal block. The total number of diagonal blocks is s and each block has 2^r distinct entries. Hence

$$s2^r \geq v-1$$

or,

$$k \geq v-1 \text{ .} \tag{5.18}$$

But 2^r divides v and 2^r divides k with $r \geq 1$. Hence

$$k = v \text{ .}$$

If $\lambda \equiv 0(\text{mod } 2^{r+1})$, every non-zero residue α that appears in one diagonal block must appear again in another diagonal block. Suppose α appears in the block defined by the shifts $x + B$ and $y + B$. Then

$$\alpha \equiv 2x + i\frac{v}{2^r} \; (\text{mod } v) \text{ ,} \tag{5.19}$$

and

$$\alpha \equiv 2y + j\frac{v}{2^r} \; (\text{mod } v) \text{ ,} \tag{5.20}$$

for some i and j between 0 and 2^r-1.

Hence,

$$2x + \frac{iv}{2^r} \equiv 2y + \frac{jv}{2^r} \quad (\text{mod } v) \text{ ,}$$

or

$$2(x - y) \equiv \frac{(j-i)v}{2^r} \quad (\text{mod } v) \text{ .}$$

If $2|(j-i)$, x and y will be in the same shift, contradicting the fact that they represent different shifts of B. Hence 2 does not divide $(j-i)$, and 2^{r+1} divides v. Moreover,

$$x \equiv y + \frac{(j-i)v}{2^{r+1}} \qquad (\text{mod } v/2) \text{ .}$$

Hence either

$$x \equiv y + \frac{(j-i)v}{2^{r+1}} \qquad (\mathrm{mod}\ v)\ ,$$

or

$$x \equiv y + \frac{(j-i)v}{2^{r+1}} + \frac{v}{2} \quad (\mathrm{mod}\ v)\ .$$

In either case, the two shifts $x + B$ and $y + B$ will differ only by $\frac{v}{2^{r+1}}$, that is

$$x + B = \left(y + \frac{v}{2^{r+1}}\right) + B\ .$$

Hence the two shifts $x + B$ and $y + B$ can be grouped together into a shift of the basic $(r+1)$-set.

Suppose there exists another diagonal block which is defined by the shift $z + B$. Let β be a non-zero residue that appears in this diagonal block. We now show that β does not appear in the blocks defined by either $x + B$ or $y + B$. Suppose β appears also in the block defined by $x + B$. Then the previous argument implies that the two shifts $x + B$ and $z + B$ differ only by $(v/2^{r+1})$. Thus the two shifts $y + B$ and $z + B$ will be identical, contrary to the choice of $z + B$. Hence the shift $z + B$ will have to pair up with yet another shift to form a shift of the basic $(r+1)$-set. Continuing in this manner, we can show that the whole set A is a union of distinct shifts of the basic $(r+1)$-set.

Let us consider the implications of Lemma 5.6. If $k = v$, the only addition set is $A = \{0, 1, \ldots, v-1\}$ which is covered by (5.11). The other alternative is an induction step. Since v is finite, there exists a maximum r such that 2^r divides v and the induction must terminate. Thus Lemma 5.6 implies that if for some $r \geq 1$, 2^r divides v and the addition set A is a union of distinct shifts of the basic r-set, then $A = \{0, 1, \ldots, v-1\}$. If k is even, the hypothesis of Lemma 5.6 is satisfied with $r = 1$, and we obtain the next theorem.

Theorem 5.7 There is no new solution for k an even integer.

Proof: Theorem 5.5 established the fact that v is even. Hence, 2^1 divides v. Moreover, if $a \in A$ and not equal to 0 or $v/2$, then $a+v/2 \in A$. The two elements a and $a + v/2$ together are a shift of the basic 1-set. Thus the elements of A, not equal to 0 or $v/2$, pair up as shifts of the basic 1-set. Now k is even which means that A has an even number of elements. Hence 0 and $v/2$ are either both in A or both not in A. In either case, A is a union of shifts of the basic 1-set. With the use of Lemma 5.6, we obtain the result that there is no new solution for k an even integer.

Let us summarize the results obtained up to this point. Theorem 5.4 implies that we only have to consider the case of λ an even integer. Theorem 5.5 implies that v is even, and if $a \in A$ and not equal to 0 or $v/2$, then $a + v/2 \in A$. Theorem 5.7 settles the case of k an even integer, and we now proceed to consider the case of k an odd integer.

Proposition 5.8 If k is odd, then either 0 or $v/2$ is in A, but not both.

Proof: Theorem 5.5 says that those a's in A not equal to 0 or $v/2$ come in pairs. Since k is odd, the number of elements of A is odd.

Hence either 0 or $v/2$ is in A but not both.

Remark 5.9 If A is a new solution, then $v/2 + A$ is again a new solution. Hence we can assume that $0 \in A$ without loss of generality.

Remark 5.10 If A is a new solution, so is the complement of A consisting of the residues modulo v that are not in A. Hence in the search for new solutions we can restrict our attention to the cases in which

$$k \leq v/2 . \qquad (5.21)$$

Proposition 5.11 Let A be a new solution with k odd and $\lambda \equiv 2 \pmod 4$. Then

$$k \geq v/2 + 1.$$

Proof: With Proposition 5.8 and Remark 5.9, we can assume that 0 is in A. Let us define a new set

$$A' = A - \{0\}.$$

Now, if $a \in A'$, then $a + v/2 \in A'$. Hence A' is a union of shifts of the basic 1-set. With suitable rearrangement of the elements in A', the addition table for A' is again a matrix of 2×2 blocks. Entries in the off diagonal blocks appear in multiples of 4, and entries in the diagonal blocks appear in multiples of 2.

Observe that the addition table for A is just the addition table for A' adjoined with an extra column and row which correspond to the 0 in A. The entries in the column also appear in the row as the addition table is symmetric. Hence, in the addition table for A, the only entries that appear with multiplicity 2 are those on the main diagonal block, or on the extra column and row.

There are a total of $(k-1)/2$ main diagonal blocks, each with 2 distinct elements. As for the extra column, there are $(k-1)$ non-zero entries. Since all other non-zero entries occur in multiples of 4 and $\lambda \equiv 2 \pmod 4$, every non-zero residue must appear in the main diagonal blocks or the extra column. Thus

$$[(k-1)/2] \times 2 + k-1 \geq v-1$$

or

$$2(k-1) \geq v-1 \; . \tag{5.22}$$

Theorem 5.5 implies that v is even. Hence (5.22) can be refined to

$$2(k-1) \geq v$$

or

$$k \geq \frac{v}{2} + 1 \; .$$

Remark 5.10 and Proposition 5.11 imply that we can assume $\lambda \equiv 0 \pmod 4$.

Theorem 5.12 Let A be a new solution with k odd, $\lambda \equiv 0 \pmod 4$, and $0 \in A$. Then

(i) $v \equiv 2 \pmod 4$, and

(ii) $d = 1$.

Proof: In the proof of Proposition 5.11, we studied the multiplicities of entries in the addition table for A. Now when $\lambda \equiv 0 \pmod 4$, the entries with multiplicity 2 must combine among themselves to give multiplicity 4. Let us consider the non-zero entries in the extra row. First of all, they are all distinct since they are exactly the entries in

A - {0}. Secondly, there are (k-1) non-zero entries in the row. Hence, all these (k-1) non-zero entries must appear as entries in the diagonal blocks. However, if $v \equiv 0 (\text{mod } 4)$, then $v/2$ is even and all the entries in the diagonal blocks are even. Hence all the non-zero entries in A are even. But then all the entries in the addition table will be even contradicting the fact that A is an addition set. Hence $v \equiv 2$ (mod 4).

Since $v \equiv 2$ (mod 4), $v/2$ is odd. Then A contains $\frac{k+1}{2}$ even elements and $\frac{k-1}{2}$ odd elements. Since v is even, we can consider the addition table modulo 2. The numbers of entries congruent to 0 modulo 2 is

$$\left(\frac{k+1}{2}\right)^2 + \left(\frac{k-1}{2}\right)^2 .$$

The number of entries congruent to 1 modulo 2 is

$$2\left(\frac{k+1}{2}\right)\left(\frac{k-1}{2}\right) .$$

However, by the remark following Corollary 5.3 we observe that d is the difference of the number of entries congruent to 0 modulo 2 and 1 modulo 2. Hence

$$d = \left(\frac{k+1}{2}\right)^2 + \left(\frac{k-1}{2}\right)^2 - 2\left(\frac{k+1}{2}\right)\left(\frac{k-1}{2}\right)$$

or

$$d = 1 .$$

Up to this point, all the results on addition sets are derived from the fact that the addition table is symmetric. To obtain further results, we will use the techniques developed in Chapter 4. Let us first summarize the results that we will need later on.

Theorem 5.13 If a new solution exists, then one exists satisfying the following conditions:

(i) $v \equiv 2 \pmod 4$,

(ii) $d = 1$, and (5.23)

(iii) $k \leq v/2$.

As in Chapter 4, we denote the Hall polynomial of an addition set by $\theta(x)$. Let ω divide v, and let $\varphi_\omega(x)$ be the ω-th cyclotomic polynomial. Let $\theta_\omega(x)$ be the remainder of $\theta(x)$ taken modulo $\varphi_\omega(x)$. Furthermore, we let $\theta_{[\omega]}(x)$ denote the remainder of $\theta(x)$ taken modulo $(x^\omega-1)$, and we let $T_\omega(x) = 1 + x + \ldots + x^{\omega-1}$.

If A is a new solution satisfying the conditions in Theorem 5.13, then its Hall polynomial satisfies

$$\theta(x)^2 \equiv 1 + \lambda T_v(x) \pmod{x^v-1}. \tag{5.24}$$

The results in Chapter 4 imply that

$$\theta_1(x) = \pm k, \text{ and} \tag{5.25}$$

$$\theta_\omega(x) = \pm 1, \tag{5.26}$$

for ω dividing v not equal to 1. Since $\theta(x)$ has non-negative coefficients,

$$\theta_1(x) = +k . \tag{5.27}$$

We now let p be an odd prime dividing v. Equation (5.24) taken modulo (x^p-1) becomes

$$\left(\theta_{[p]}(x)\right)^2 \equiv 1 + \frac{\lambda v}{p} T_p(x) \pmod{x^p-1}.$$

Observe that $\theta_{[p]}(x)$ again has integral coefficients. Using the constructions of Chapter 4, $\theta_{[p]}(x)$ is determined by $\theta_1(x)$ and $\theta_p(x)$. With the fact that $\theta_1(x) = +k$, there are only two possibilities for $\theta_{[p]}(x)$. The restriction that it has integral coefficients will give us a condition on the sign of $\theta_p(x)$.

Theorem 5.14 If A is a new solution satisfying the conditions in (5.23) and p is an odd prime dividing v, then

$$\theta_p(x) = \left\{ \begin{array}{ll} +1 & \text{when p divides } (k-1) \\ -1 & \text{when p divides } (k+1) \end{array} \right\} . \qquad (5.28)$$

Proof: We will use equations (4.17) and (4.18) to construct $\theta_{[p]}(x)$. It is easy to calculate that

$$B_{p,1}(x) = T_p(x)$$

and that

$$B_{p,p}(x) = p - T_p(x).$$

If $\theta_p(x) = +1$, then

$$\theta_{[p]}(x) = 1 + (\frac{k-1}{p})T_p(x) \ . \qquad (5.29)$$

If $\theta_p(x) = -1$, then

$$\theta_{[p]}(x) = -1 + (\frac{k+1}{p})T_p(x). \qquad (5.30)$$

Since p is an odd prime, (5.29) and (5.30) cannot both have integral coefficients. However, as

$$(k+1)(k-1) = \lambda v,$$

any odd prime dividing v will divide either $k+1$ or $k-1$. If p divides $k+1$, then $\theta_{[p]}(x)$ is given by (5.30) and $\theta_p(x) = -1$. If p divides $k-1$, $\theta_{[p]}(x)$ is given by (5.29) and $\theta_p(x) = 1$.

Carrying the construction one step further, we obtain the following result.

Theorem 5.15 If A is a new solution satisfying the conditions in (5.23), then $v/2$ divides either $k-1$ or $k+1$.

Proof: Condition (i) of (5.23) implies that $v/2$ is odd. Let p be an odd prime dividing $v/2$. Then p divides either $k-1$ or $k+1$. Suppose p divides $k-1$. We will show that $v/2$ divides $k-1$.

Assume that there exists another odd prime q dividing $v/2$ such that q divides $k+1$. We now consider the possibilities for $\theta_{[pq]}(x)$, which has integral coefficients. A little calculation gives

$$B_{pq,\,1}(x) = T_{pq}(x),$$

$$B_{pq,\,p}(x) = p\left(\frac{x^{pq}-1}{x^{p}-1}\right) - T_{pq}(x),$$

$$B_{pq,\,q}(x) = q\left(\frac{x^{pq}-1}{x^{q}-1}\right) - T_{pq}(x)\,,$$

and

$$B_{pq,\,pq}(x) = T_{pq}(x) + pq - p\left(\frac{x^{pq}-1}{x^{p}-1}\right) - q\left(\frac{x^{pq}-1}{x^{q}-1}\right).$$

Since p divides $k-1$ by Theorem 5.14, we have $\theta_p(x) = 1$. Similarly $\theta_p(x) = -1$. Since $\theta_1(x)$ is equal to k, the only choice in the formula (4.17) is in the sign of $\theta_{pq}(x)$. If $\theta_{pq}(x) = 1$, then

$$\theta_{[pq]}(x) = 1 + \frac{k+1}{pq} T_{pq}(x) - \frac{2}{p} \sum_{i=0}^{p-1} (x^q)^i.$$

If $\theta_{pq}(x) = -1$, then

$$\theta_{[pq]}(x) = -1 + \frac{k-1}{pq} T_{pq}(x) - \frac{2}{q} \sum_{i=0}^{q-1} (x^p)^i.$$

However, pq does not divide k+1 or k-1. Hence $\theta_{[pq]}(x)$ cannot have integral coefficients, which is a contradiction.

Thus, if there exists an odd prime divisor of v/2 that divides k-1, then all the odd prime divisors of v/2 divide k-1. Hence v/2 is co-prime to k+1. But since $(k+1)(k-1) = \lambda v$, we find that v/2 divides k-1.

On the other hand, if there does not exist an odd prime divisor of v/2 that divides k-1, then v/2 is co-prime to k-1 and v/2 divides k+1.

Finally, we can prove that there are no new solutions.

<u>Theorem 5.16</u> The list (5.11) contains all of the addition sets.

Proof: We have shown that if a new solution exists, then one exists that satisfies all the conditions in (5.23). Theorem 5.15 implies that v/2 divides either k-1 or k+1.

If v/2 divides k+1, then we have

$$k+1 \geq v/2 . \tag{5.31}$$

Since k and v/2 are both odd, (5.31) implies that

$$k \geq v/2 .$$

With condition (iii) of (5.23), we have

$$k = v/2 .$$

Since $k^2 = 1 + \lambda v$, we have

$$v^2 = 4 + 4 \lambda v . \tag{5.32}$$

The only integral solutions of (5.32) are $\lambda = 0$ and $v = \pm 2$. The addition sets with these parameters are included in (5.11).

If $v/2$ divides $k-1$, then either $k=1$ or

$$k-1 \geq v/2 . \tag{5.33}$$

The addition sets with $k=1$ are included in (5.11). Relation (5.33) contradicts condition (iii) of (5.23). This finishes our proof.

In the next chapter, we will look at a generalization of addition sets. Since the generalization will include all the difference sets, there will be non-trivial solutions.

Chapter 6

(v, k, λ, g) - ADDITION SETS

In Chapter 5, we considered (0, 1) 1-circulants satisfying the matrix equation

$$A^2 = dI + \lambda J , \qquad (6.1)$$

and we have shown that the existence of such matrices is connected with the existence of addition sets. In this chapter, we will consider (0, 1) g-circulants satisfying (6.1). These matrices correspond to a generalized version of addition sets.

A (v, k, λ, g)-addition set $A = \{a_1, a_2, \ldots, a_k\}$, or simply a g-<u>addition set,</u> is a collection of k distinct residues modulo v, such that for any residue $\alpha \not\equiv 0 \pmod{v}$ the congruence

$$a_i + ga_j \equiv \alpha (\text{mod } v) \qquad (6.2)$$

has exactly λ solution pairs (a_i, a_j) with a_i and a_j in A. Furthermore, we require that

$$k \geq 1 . \qquad (6.3)$$

It should be pointed out that when $g = -1$, the (-1)-addition sets are the previously defined difference sets, and when $g = 1$, the 1-addition sets are those studied in Chapter 5.

<u>Remark 6.1</u> Again, it can be easily seen that every g-addition set corresponds to a (0, 1) g-circulant satisfying $A^2 = dI + \lambda J$. Given a g-addition set A, we can define the first row of a g-circulant matrix A by placing 1's in each of the a_i-th positions, where the a_i's

belong to the g-addition set A. The complete g-circulant is then obtained by shifting. Conversely, given a (0, 1) g-circulant A satisfying (6.1), we can form a g-addition set from the first row of A.

We can define a Hall polynomial $\theta(x)$ for a g-addition set A by

$$\theta(x) = \sum_{i=1}^{k} x^{a_i}, \quad a_i \in A. \tag{6.4}$$

Observe that

$$\begin{aligned}\theta(x)\,\theta(x^g) &= \sum_{i,j=1}^{k} x^{a_i+ga_j} \\ &= d + \lambda T(x) \pmod{x^v-1}.\end{aligned} \tag{6.5}$$

One can prove some elementary results about (v, k, λ, g)-addition sets.

Theorem 6.2 If $d \neq 0$, then $g^2 \equiv 1 \pmod{v}$.

Proof: We have seen that a (v, k, λ, g)-addition set corresponds to a (0, 1) g-circulant satisfying $A^2 = dI + \lambda J$. Using conclusion (i) of Theorem 3.1, we obtain Theorem 6.2.

The multiplier theorem is important in the study of difference sets and a similar result can be proved for g-addition sets. Let us first make some definitions.

Let A be a (v, k, λ, g)-addition set. Define

$$A + x = \{a + x \mid a \in A\} \tag{6.6}$$

for each residue x modulo v. Then A + x is called a shift of A. If A is a (v, k, λ, g)-addition set and x is any residue modulo v, define

$$xA = \{xa \mid a \in A\}. \qquad (6.7)$$

If xA is a shift of A, then x is a multiplier of A. In particular, if $xA = A$, then x fixes A.

The trivial multiplier 1 always fixes a g-addition set. The following theorem is a generalization of the multiplier theorem for difference sets to addition sets. The proof is very similar to the original one given for difference sets. (Hall and Ryser [1951]).

Theorem 6.3 If $A = \{a_1, a_2, \ldots, a_k\}$ is a (v, k, λ, g)-addition set, where $k^2 = d + \lambda v$, and if p is a prime dividing d such that $(p, v) = 1$ and $p > \lambda$, then p is a multiplier of the g-addition set.

Proof: Since A is a g-addition set, its Hall polynomial satisfies

$$\theta(x)\theta(x^g) \equiv d + \lambda T(x) \pmod{x^v - 1}. \qquad (6.8)$$

Observe that if $f(x)$ is an arbitrary polynomial with integral coefficients, then

$$f(x)T(x) \equiv f(1)T(x) \pmod{x^v - 1}. \qquad (6.9)$$

By hypothesis p divides d but not v. Also $p > \lambda$ and $k^2 = d + \lambda v$. This implies p does not divide k. Thus

$$k^{p-1} \equiv 1 \pmod{p}. \qquad (6.10)$$

Since all the binomial coefficients $\binom{p}{i}$, where $i = 1, 2, \ldots p-1$, are divisible by p, we have

$$\theta(x)^p \equiv \theta(x^p) \pmod{p}. \qquad (6.11)$$

We now multiply (6.8) by $\theta(x)^{p-1}$ and apply (6.9), (6.10) and (6.11). The resulting relationship is

$$\theta(x^p)\,\theta(x^g) \equiv \lambda T(x) + pR(x) \pmod{x^v - 1}, \qquad (6.12)$$

where R(x) is a polynomial with integral coefficients. Puting $x = 1$ in (6.12), we get

$$k^2 = \lambda v + pR(1).$$

Thus

$$pR(1) = d. \qquad (6.13)$$

We now have four relations

$$\begin{aligned} &\theta(x)\,\theta(x^g) \equiv d + \lambda T(x) \pmod{x^v - 1}, \\ &\theta(x^p)\theta(x^{gp}) \equiv d + \lambda T(x) \pmod{x^v - 1}, \\ &\theta(x^p)\,\theta(x^g) \equiv \lambda T(x) + pR(x) \pmod{x^v - 1}, \text{ and} \\ &\theta(x^{gp})\theta(x) \equiv pR(x^g) + \lambda T(x) \pmod{x^v - 1}. \end{aligned} \qquad (6.14)$$

The first of these is (6.8). The second uses the fact that pA is again a g-addition set, since p is prime to v. The third one is (6.12), and the fourth one is obtained by putting x^g in (6.12), and observing that

$$g^2 \equiv 1 \pmod{v},$$

$$T(x^g) \equiv T(x) \pmod{x^v - 1}$$

and

$$x^{vg} - 1 = (x^v - 1)(x^{v(g-1)} + x^{v(g-2)} + \dots + 1).$$

In (6.14), the product of the left sides of the first two congruences is the same as the product of the third and fourth. Hence

$$\{\lambda\, T(x) + pR(x)\}\ \{\lambda\, T(x) + pR(x^g)\} \equiv (d+\lambda T(x))^2 \pmod{x^v - 1}. \tag{6.15}$$

Now, using $pR(1) = d$, together with (6.9), we see that (6.15) simplifies to

$$p^2 R(x) R(x^g) \equiv d^2 \pmod{x^v - 1}\ . \tag{6.16}$$

The expression $\theta(x^p)\,\theta(x^g)$ of (6.12) regarded as a polynomial of degree less than v has non-negative integral coefficients. Now $p > \lambda$, and this implies that $R(x)$ in (6.12) has non-negative coefficients. The structure of (6.16) implies that $R(x)$ cannot have more than one positive term. Hence, $R(x)$ is a monomial, (say wx^s), and

$$pR(x) \equiv pwx^s \equiv dx^s \pmod{x^v - 1}\ . \tag{6.17}$$

We now multiply (6.11) by $\theta(x)$ and apply (6.8), (6.9) and (6.17). This gives

$$d\theta(x^p) \equiv dx^s\ \theta(x) \pmod{x^v - 1}\ .$$

Dividing by d,

$$\theta(x^p) \equiv x^s\, \theta(x) \pmod{x^v - 1}\ , \tag{6.18}$$

which implies that p is a multiplier.

Remark 6.4 Observe that since $R(x)$ is a monomial, by substituting it into (6.16) we get

$$p^2 w^2 x^{s+gs} \equiv d^2 \pmod{x^v - 1}\ .$$

Hence,

$$v \mid s(g+1)\ . \tag{6.19}$$

The multiplier theorem is useful in constructing difference sets. It is hoped that new g-addition sets can also be constructed.

Next we consider some examples of (v, k, λ, g)-addition sets. The following result was first reported in Ryser [1970].

Theorem 6.5 If $k^2 = 1 + \lambda v$, then the set $A = \{0, 1, \ldots, k-1\}$ is a (v, k, λ, k)-addition set with $d = 1$.

Proof: Let $\theta(x)$ be the Hall polynomial for A. Then

$$\theta(x)\ \theta(x^k) = 1 + x + \ldots + x^{k^2-1}. \tag{6.20}$$

Equation (6.20) taken modulo (x^v-1) becomes

$$\theta(x)\theta(x^k) \equiv 1 + \lambda(1 + x + \ldots + x^{v-1}) \pmod{x^v-1}. \tag{6.21}$$

Hence A is a (v, k, λ, k)-addition set with $d = 1$.

Remark 6.6 In the case of difference sets, it is well known that -1 is never a multiplier of a non-trivial difference set. (Johnsen [1964], Brualdi [1965] and Yates [1967]). Let us consider the (8, 3, 1, 3)-addition set constructed in Theorem 6.5. It can be easily checked that -1 is the only non-trivial multiplier for this 3-addition set.

Theorem 6.7 Let A be a (v, k, λ, g)-addition set with $d \neq 0$. Then it is also a (v, k, λ, h)-addition set if and only if gh is a multiplier fixing A.

Proof: Assume that A is both a g- and an h-addition set. Then

$$\theta(x)\theta(x^g) \equiv d + \lambda T(x) \quad \pmod{x^v-1}, \tag{6.22}$$

and

$$\theta(x)\theta(x^h) \equiv d + \lambda T(x) \quad (\text{mod } x^v - 1) . \tag{6.23}$$

Substituting x^h for x in (6.22), we obtain

$$\theta(x^h)\theta(x^{gh}) \equiv d + \lambda T(x^h) \quad (\text{mod } x^{vh} - 1) . \tag{6.24}$$

However, we have $(x^v - 1)$ dividing $(x^{vh} - 1)$, and $T(x^h) \equiv T(x) (\text{mod } x^v - 1)$. Hence, (6.24) implies

$$\theta(x^h)\theta(x^{gh}) \equiv d + \lambda T(x) \quad (\text{mod } x^v - 1) . \tag{6.25}$$

Multiplying (6.25) by $\theta(x)$, we have

$$\theta(x)\theta(x^h)\theta(x^{gh}) \equiv \theta(x) (d + \lambda T(x)) \ (\text{mod } x^v - 1) .$$

Using (6.23), we have

$$(d + \lambda T(x))\, \theta(x^{gh}) \equiv \theta(x)\ (d + \lambda T(x)) \ \ (\text{mod } x^v - 1) .$$

Observing that

$$\theta(x^i)T(x) \equiv kT(x) \quad (\text{mod } x^v - 1) ,$$

for any i, we have

$$d\ \theta(x^{gh}) + \lambda kT(x) \equiv d\ \theta(x) + \lambda kT(x) \ \ (\text{mod } x^v - 1) . \tag{6.26}$$

If $d \neq 0$, (6.26) implies that

$$\theta(x^{gh}) \ \equiv \ \theta(x) \qquad (\text{mod } x^v - 1) ,$$

which is the same as saying that gh is a multiplier fixing A.

Next we assume that A is a g-addition set with gh as a multiplier fixing A. Then

$$\theta(x)\,\theta(x^g) \equiv d + \lambda T(x) \pmod{x^v - 1}\,. \tag{6.27}$$

Since gh is a multiplier fixing A, $\theta(x) \equiv \theta(x^{gh}) \pmod{x^v-1}$. Hence

$$\theta(x^{gh})\,\theta(x^g) \equiv d + \lambda T(x) \pmod{x^v - 1}. \tag{6.28}$$

Substituting x^g for x in (6.28), we have

$$\theta(x^{g^2 h})\,\theta(x^{g^2}) \equiv d + \lambda T(x^g) \pmod{x^{vg} - 1}\,. \tag{6.29}$$

We now use the fact that $d \neq 0$ implies $g^2 \equiv 1 \pmod{v}$, that (x^v-1) divides $(x^{vg}-1)$ and that $T(x^g) \equiv T(x) \pmod{x^v-1}$. Equation (6.29) then implies that

$$\theta(x^h)\theta(x) \equiv d + \lambda T(x) \pmod{x^v - 1}\,,$$

which means that A is also an h-addition set.

Corollary 6.8 A (v, k, λ)-difference set is also a (v, k, λ, g)-addition set if $-g$ fixes A.

Corollary 6.8 implies the existence of many (v, k, λ, g)-addition sets. The following is a list of those with $g \neq -1$ and $v < 50$.

v	k	λ	g	d	A
15	7	3	11	4	{0, 1, 2, 4, 5, 8, 10}
21	5	1	13	4	{3, 6, 7, 12, 14}
35	17	8	6	9	{0, 1, 3, 4, 7, 9, 11, 12, 13, 14, 16, 17, 21, 27, 28, 29, 33}
40	13	4	31	9	{1, 2, 3, 5, 6, 9, 14, 15, 18, 20, 25, 27, 35}

There is still much that can be done concerning g-addition sets. The following are some suggestions.

1) Construct solutions with $d \neq 0, 1,$ or $k-\lambda$.

2) Find more non-existence results.

3) Search for all possible g-addition sets for, say, $v \leq 100$.

4) Generalize the notion of g-addition sets to the notion of g-addition sets over an abelian group.

REFERENCES

Ablow, C. M., and Brenner, J. L.

1963 "Roots and Canonical Forms for Circulant Matrices," Trans. Amer. Math. Soc. 107, 360-376.

Baumert, L. D.

1971 Cyclic Difference Sets, Lecture Notes in Mathematics, Vol. 182, Springer-Verlag.

Berggren, J. L.

1962 "An algebraic characterization of symmetric graphs with a prime number of vertices," Bull. Aust. Math. Soc. 7, 131-134.

Brualdi, R. A.

1965 "A Note on Multipliers of Difference Sets," J. Res. Nat. Bus. Standards, Sect. B 698, 87-89.

Elspas, B., and Turner, J.

1970 "Graphs with Circulant Adjacency Matrices," J. Comb. Theory 9, 297-307.

Hall, M., and Ryser, H. J.

1951 "Cyclic Incidence Matrices," Canad. J. Math. 3, 495-502.

Hoffman, A. J., and Singleton, R. R.

1960 "On Moore Graphs with Diameters 2 and 3," I. B. M. J. Res. Develop. 4, 497-504.

Johnsen, E. C.

1964 "The Inverse Multiplier for Abelian Group Difference Sets," Canad. J. Math. 16, 787-796.

References (Continued)

Knuth, D. E.

1970 "Notes on central groupoids," J. Comb. Theory 8, 376-390.

Lang, S.

1965 Algebra, Addison-Wesley

Ryser, H. J.

1970 "A Generalization of the Matrix Equation $A^2 = J$," Lin. Alg. and its Appl. 3, 451-460.

Tuero, M.

1961 "A contribution to the Theory of Cyclic Graphs," Matrix and Tensor Quart., 74-80.

Turner, J.

1967 "Point-Symmetric Graphs with a Prime Number of Points," J. Comb. Theory 3, 136-145.

Yates, D. L.

1967 "Another Proof of a Theorem on Difference Sets," Proc. Cambridge Philos. Soc. 63, 595-596.