

A TABLE FOR PARTIAL DIFFERENCE SETS IN ABELIAN GROUPS

A UROPS report submitted by

MOK HOI NAM

SUPERVISOR: A/P MA SIU LUN

DEPARTMENT OF MATHEMATICS
NATIONAL UNIVERSITY OF SINGAPORE

2003/2004

Acknowledgements

Foremost, I would like to thank my supervisor A/P Ma Siu Lun for teaching and guiding me throughout the span of this project. He has taken great efforts in assisting my understanding of the subject material, and suggested numerous improvements to my drafts. This project would not have been achievable without his guidance. I am immensely grateful to him for sharing the joy of mathematics with me.

I would like to extend my heartfelt thanks to my family members for their kind words of encouragement and support, as well as the Special Programme in Science, which had provided me this opportunity to pursue this project. I am also in debt to the SPS community and computer cluster in providing a conducive environment for me to complete the report. My greatest thanks goes to Mr Kelken Chang who had taught me \LaTeX with utmost patience, and therefore enabling me to typeset this report. Last but not least, I would take this opportunity to say a big 'thank you' to Shruti, Gaurav, Huegesh, Valerie, Yukti and all my other friends.

MOK HOI NAM

OCTOBER 2003

Contents

Acknowledgements	iii
Abstract	vii
1 Introduction	1
1.1 Partial Difference Sets	1
1.2 Notation and Terminology	2
1.3 Basic Properties	3
2 Character Values and Duals of PDS	9
2.1 Abelian Characters	9
2.2 Fourier Inversion Formula	11
2.3 Character Values of PDS	13
2.4 Some Number Theory	16
3 Examples of Regular PDS	19
3.1 Paley PDS	19
3.2 PCP	20

4	Table of Parameters	23
4.1	Conditions	23
4.2	Table of Parameters	26
A	Examples of PDS	29
A.1	Examples	29
A.2	Some more non-existence theorems	30
B	C Program	33
	Bibliography	44

Abstract

Let G be a group of order v and D be a subset of G with k elements such that $D \neq \emptyset$, $\{e\}$, $G \setminus \{e\}$, and G . Then D is called a (v, k, λ, μ) -partial difference set (PDS) in G if the expressions gh^{-1} , for g and h in D with $g \neq h$, represent each nonidentity element in D exactly λ times and represent each nonidentity element not in D exactly μ times.

With the definition of partial difference sets, the aim of this project is to generate a table for partial difference sets in abelian groups. The study of partial difference sets began as early as 1965, and is closely related to the studies of strongly regular graphs and two-weight codes.

In the first chapter, we provide some preliminary definitions and terminology required, including the group ring notation. Next, some basic properties of partial differences sets and also some simple conditions on their parameters for the existence of regular PDS are also given.

The second chapter introduces abelian characters and also the usage of the Fourier Inversion Formula in obtaining the character values of PDS. Finite Fourier Transform, an important tool in the study of PDS, is given as well. The third section of this chapter illustrates how character values can enable us to detect PDS, and proves that the dual D^+ of D is also a PDS. The Gauss sum is also stated as a preliminary for the study of regular Paley PDS in chapter 3.

In chapter 3, we give two examples of regular PDS, namely, Paley PDS and partial congruence partitions. The proofs of these two examples are given as well, and also the parameters of PDS which fall into these two categories. The existence of PCPs in abelian group G of order n^2 , which belong to the Latin square type, is also stated without proof. We refer the reader to further examples and theorems regarding non-existence of certain PDS in the Appendix.

In chapter 4, a list of conditions and restrictions on the parameters $(v, k, \lambda, \mu, \beta, \Delta)$ of PDS is given. The parameters generated for the table 4.2 in this chapter are with $v < 200$, and the other parameters are subsequently calculated with the formulae stated. If D is a nontrivial abelian regular PDS, then the complement $D' = (G \setminus D) \setminus \{e\}$ and the dual D^+ of D given in chapter 3, both of which are regular PDS, are omitted from the table.

The table 4.2 in chapter 4 gives the values of the parameters $v, k, \lambda, \mu, \beta$ and Δ , together with an example or remark, stating what type of PDS the set of parameters fall under, or whether it is non-existent, or the existence of the PDS is unknown. There are altogether 80 sets of parameters, for $v < 200$, with 9 unknowns. Most of the parameters generated are of the type Paley and PCP, and there are more unknowns as v increases.

In Appendix A, we give several examples of PDS such as PDS from reversible difference sets and PDS from the 8th cyclotomic classes in \mathbb{F}_3^4 . We also present two theorems giving the non-existence of PDS with certain parameters.

Appendix B contains the C program used to generate the table 4.2. The C program has nine functions in which the conditions and restrictions are tested on the parameters. The first function *find_para* makes use of the equation (4.2) to generate all the possibilities of the parameters within $v < 200$. The program is written in a flexible manner such that the user can enter a limit for the value of v , and thus values of $v > 200$ can be generated. Also, restrictions on the parameters k and μ makes sure that there is no redundancy in the generation of parameters.

The functions *conditions* and *conditions2* implement the formulae in section 4.1, and eliminates all the parameters that do not fit the conditions. The dual and complement of a partial difference set are further omitted from the table. The *comp_prime* and *factorise* functions are called in the previous mentioned functions so that they can compare primes and also factorise a number into their respective prime powers. Lastly, the functions *find_eg*, *t15_1* and *t2_2* put in the examples/remarks column in the table and ??? is placed if the existence of the parameters is unknown.

Statement of author's contributions

Most of the basics and theorems were taught by my supervisor and some of the proofs obtained from K.M.Ng, 1994, [4]. Through my own understanding of the topic, most of the proofs in Chapter 1 were written by me. In Chapter 4, the conditions and restrictions of the parameters were obtained from the references and then the C program was written to generate the table of parameters. (table 4.2) This table is similar to the table found in S.L. Ma, 1994, [3], except that this table was generated with starting value of v instead of k . This enables us to see the total number of different PDS for a certain group size. Also, some restrictions of the parameters found in other references were placed into this table.

Introduction

This chapter defines partial difference sets, states certain notation and terminology, and also studies some of the basic properties of partial difference sets, together with some of the restrictions of their parameters.

1.1 Partial Difference Sets

Partial difference sets were named by I.M. Chakravarti, 1969 [1], but introduced by Bose and Cameron, 1965 [2] in their studies of calibration designs and the bridge tournament problem. The study of partial difference sets is closely related to the studies of strongly regular graphs and two-weight codes.

Definition 1.1.1 Let G be a group of order v and D be a subset of G with k elements such that $D \neq \emptyset$, $\{e\}$, $G \setminus \{e\}$, and G . Then D is called a (v, k, λ, μ) -partial difference set (PDS) in G if the expressions gh^{-1} , for g and h in D with $g \neq h$, represent each nonidentity element in D exactly λ times and represent each nonidentity element not in D exactly μ times. A PDS D is called *abelian* (resp. *non-abelian*) if the group G is *abelian* (resp. *non-abelian*).

Example 1.1.1 Let $G = \langle a, b \mid a^2 = b^2 = 1, ab = ba \rangle$, and $D = \{a, b\}$. Then D is a $(4, 2, 0, 2)$ -partial difference set in G . (Refer to the table below)

Elements	a	b
a	1	ab
b	ab	1

Example 1.1.2 Let $G = \{a \mid a^7 = 1\}$ and $D = \{a, a^2, a^4\}$.

Then D is a $(7, 3, 1, 1)$ -partial difference set in G . (Refer to the table below)

Elements	a	a^2	a^4
a	1	a^6	a^4
a^2	a	1	a^5
a^4	a^3	a^2	1

Definition 1.1.2 Let D be a PDS. If $e \notin D$ and $D^{(-1)} = D$, then D is said to be regular.

Example 1.1.3 Let G be a group of order v and H be a proper subgroup of G with order w . Then $H \setminus \{e\}$ is a regular $(v, w - 1, w - 2, 0)$ -PDS.

1.2 Notation and Terminology

In the following, G is a finite group, of order v and e is the identity of G . The group operation is written multiplicatively. Usually, the study of partial difference sets is carried out using the group ring $R[G]$ where $R = \mathbb{Z}$ or \mathbb{C} . It is defined as follows:

Definition 1.2.1 Let $G = \{g_1, g_2, \dots, g_v\}$ and R be a commutative ring with identity $1 \neq 0$. The group ring, $R[G]$, of G is defined to be the set of all formal sums

$$a_1g_1 + a_2g_2 + \dots + a_vg_v \quad \text{where} \quad a_i \in R, 1 \leq i \leq v.$$

The element $1g$ for $g \in G$ is written simply as g .

Addition in the group ring is defined as follows:

$$\sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g) g$$

and multiplication as

$$\left(\sum_{g \in G} a_g g \right) \left(\sum_{g \in G} b_g g \right) = \sum_{g \in G} \left(\sum_{g_1 g_2 = g} a_{g_1} b_{g_2} \right) g.$$

With these two operations, $R[G]$ is a ring. Also, the ring $R[G]$ is commutative if G is abelian. For any integer t and $y = \sum_{g \in G} a_g g \in R[G]$, let $y^{(t)} = \sum_{g \in G} a_g g^t$.

Let D be any non-empty subset of G . The notation \overline{D} is used to denote the element $\sum_{g \in D} g$ in $R[G]$. Thus, \overline{D} has coefficient 1 on those group elements in D and coefficient 0 on those group elements not in D . Also, for any integer t , we define $D^{(t)}$ to be the set $\{g^t \mid g \in D\}$.

Definition 1.2.2 A subset D of a group G is *trivial* if either $D \cup \{e\}$ or $(G \setminus D) \cup \{e\}$ is a subgroup of G . Otherwise, D is said to be *non-trivial*.

1.3 Basic Properties

Proposition 1.3.1 If D is a (v, k, λ, μ) -PDS with $\lambda \neq \mu$, then $D^{(-1)} = D$.

Proof:

For any $g \in G \setminus \{e\}$, $g_1 g_2^{-1} = g$ if and only if $g_2 g_1^{-1} = g^{-1}$, where $g_1, g_2 \in G$. Hence, for $x, y \in D$, the number of solution pairs (g_1, g_2) for the equation $g_1 g_2^{-1} = g$ is equal to the number of solution pairs (g_1, g_2) for the equation $g_1 g_2^{-1} = g^{-1}$.

Let $d \in D$, $d \neq e$, and for $x, y \in D$, the number of times in which (x, y) represent d^{-1} is λ . Since $\lambda \neq \mu$, d^{-1} is in D . Therefore, $D^{(-1)} \subset D$. Similarly, $D \subset D^{(-1)}$, thus $D^{(-1)} = D$. \square

Theorem 1.3.1 Let G be a group of order v and D be a subset of G with k elements. Then D is a (v, k, λ, μ) -PDS in G if and only if

$$\overline{D} \overline{D}^{(-1)} = \mu \overline{G} + (\lambda - \mu) \overline{D} + \gamma e \quad (1.1)$$

where $\gamma = k - \mu$ if $e \notin D$ and $\gamma = k - \lambda$ if $e \in D$. If $D^{(-1)} = D$, then

$$\overline{D}^2 = \mu\overline{G} + (\lambda - \mu)\overline{D} + \gamma e \quad (1.2)$$

and

$$(2\overline{D} - \beta e)^2 = 4\mu\overline{G} + \Delta e \quad (1.3)$$

where $\beta = \lambda - \mu$ and $\Delta = \beta^2 + 4\gamma$.

Proof:

(Necessity) Assume that D is a (v, k, λ, μ) -PDS in G . Suppose $e \notin D$. Then if $D = \{d_1, d_2, \dots, d_k\}$, we have

$$\begin{aligned} \overline{DD}^{(-1)} &= (d_1 + d_2 + \dots + d_k)(d_1^{-1} + d_2^{-1} + \dots + d_k^{-1}) \\ &= ke + \sum_{i \neq j} d_i d_j^{-1} \\ &= ke + \lambda\overline{D} + \mu(\overline{G} - \overline{D} - e) \\ &= (k - \mu)e + (\lambda - \mu)\overline{D} + \mu\overline{G} \\ &= \mu\overline{G} + (\lambda - \mu)\overline{D} + (k - \mu)e \end{aligned}$$

Similarly, if $e \in D$, then

$$\begin{aligned} \overline{DD}^{(-1)} &= (e + d_1 + d_2 + \dots + d_{k-1})(e + d_1^{-1} + d_2^{-1} + \dots + d_{k-1}^{-1}) \\ &= ke + \sum_{i \neq j} d_i d_j^{-1} \\ &= ke + \lambda(\overline{D} - e) + \mu(\overline{G} - \overline{D}) \\ &= (k - \lambda)e + (\lambda - \mu)\overline{D} + \mu\overline{G} \\ &= \mu\overline{G} + (\lambda - \mu)\overline{D} + (k - \lambda)e \end{aligned}$$

(Sufficiency) Suppose $e \notin D$ and $\overline{DD}^{(-1)} = \mu\overline{G} + (\lambda - \mu)\overline{D} + (k - \mu)e$. Then

$$ke + \sum_{i \neq j} d_i d_j^{-1} = ke + \lambda\overline{D} + \mu(\overline{G} - \overline{D} - e)$$

and hence

$$\sum_{i \neq j} d_i d_j^{-1} = \lambda \bar{D} + \mu(\bar{G} - \bar{D} - e)$$

Therefore, the expressions gh^{-1} for $g, h \in D$ with $g \neq h$ represent each element in D exactly λ times and represent each non-identity element not in D exactly μ times. Thus, D is a (v, k, λ, μ) -PDS in G .

For the case when $e \in D$ and $\overline{DD}^{(-1)} = \mu\bar{G} + (\lambda - \mu)\bar{D} + (k - \lambda)e$,

$$ke + \sum_{i \neq j} d_i d_j^{-1} = ke + \lambda(\bar{D} - e) + \mu(\bar{G} - \bar{D})$$

and therefore

$$\sum_{i \neq j} d_i d_j^{-1} = \lambda(\bar{D} - e) + \mu(\bar{G} - \bar{D})$$

Therefore, the expressions gh^{-1} for $g, h \in D$ with $g \neq h$ represent each non-identity element in D exactly λ times and represent each element not in D exactly μ times. Thus, D is a (v, k, λ, μ) -PDS in G .

Since $D^{(-1)} = D$, we have $\bar{D}^{(-1)} = \bar{D}$. Therefore,

$$\begin{aligned} \bar{D}^2 &= \overline{DD}^{(-1)} \\ &= \mu\bar{G} + (\lambda - \mu)\bar{D} + \gamma e. \end{aligned}$$

Also, we have

$$\begin{aligned} (2\bar{D} - \beta e)^2 &= 4\bar{D}^2 - 4\beta\bar{D} + \beta^2 e \\ &= 4\mu\bar{G} + 4(\lambda - \mu)\bar{D} + 4\gamma e - 4\beta\bar{D} + \beta^2 e \\ &= 4\mu\bar{G} + \Delta e. \quad \square \end{aligned}$$

The parameters β and Δ in Theorem 1.3.1 are very important in the study of PDSs.

Proposition 1.3.2 If D is a (v, k, λ, μ) -PDS with $e \in D$, then $D \setminus \{e\}$ is also a PDS.

Proof:

Using the above theorem, with $\overline{D}_1 = (\overline{D} - e)$,

$$\begin{aligned}
\overline{D}_1 \overline{D}_1^{(-1)} &= (\overline{D} - e)(\overline{D} - e)^{(-1)} \\
&= (d_1 + d_2 + \cdots + d_k - e)(d_1^{-1} + d_2^{-1} + \cdots + d_k^{-1} - e) \\
&= \overline{D}^2 - 2\overline{D} + e \\
&= \lambda\overline{D} - 2\overline{D} + \mu(\overline{G} - \overline{D} - e) + (k - e) \\
&= (k - e) + (\lambda - 2)\overline{D} + \mu(\overline{G} - \overline{D} - e) \\
&= (k - \mu - e) + (\lambda - 2 - \mu)\overline{D} + \mu(\overline{G})
\end{aligned}$$

Hence if D has parameters $(v, k, \lambda, \mu, \beta, \Delta)$, then $D_1 = D \setminus \{e\}$ has parameters

$$(v_1, k_1, \lambda_1, \mu_1, \beta_1, \Delta_1) = (v, k - 1, \lambda - 2, \mu, \beta - 2, \Delta).$$

Using similar methods as the above proposition, we can see that if D is a regular (v, k, λ, μ) -PDS, $G \setminus D$ is a $(v, v - k, v - 2k + \mu, v - 2k - \lambda)$ -PDS. Also, $(G \setminus D) \setminus \{e\}$ is also a PDS with parameters $(v, v - k - 1, v - 2k - 2 + \mu, v - 2k + \lambda)$. \square

The following are some simple conditions on the parameters for the existence of regular PDS.

Proposition 1.3.3 The parameters of a regular (v, k, λ, μ) -PDS satisfy

- (a) $(v + \beta)^2 - (\Delta - \beta^2)(v - 1)$ must be a square;
- (b) $k = \left[(v + \beta) \pm \sqrt{(v + \beta)^2 - (\Delta - \beta^2)(v - 1)} \right] / 2$;
- (c) β and Δ have the same parity; and
- (d) if $D \neq \emptyset$ and $G \setminus \{e\}$, then $0 \leq \lambda \leq k - 1$ and $0 \leq \mu \leq k$.

Proof:

- (a) From (1.2), counting the terms of LHS and RHS, we have $k^2 = \mu v + (\lambda - \mu)k + \gamma$.

Therefore,

$$\begin{aligned}
k &= \frac{(v + \beta) \pm \sqrt{(v + \beta)^2 - 4(v - 1)\gamma}}{2} \\
&= \frac{(v + \beta) \pm \sqrt{(v + \beta)^2 - (\Delta - \beta^2)(v - 1)}}{2}.
\end{aligned}$$

If $(v + \beta)^2 - (\Delta - \beta^2)(v - 1)$ is not a square, then k will not be an integer.

(b) As shown in part (a).

(c) If β is even (respectively odd), then $\Delta = \beta^2 + 4\gamma$ is even (respectively odd).

(d) Let $d \in D$. Consider $xy^{-1} = d$, where $x, y \in D$, and thus, $x = dy$. Since D is regular, $x \neq e$, so $y \in D \setminus \{d^{-1}\}$. Therefore, $0 \leq \lambda \leq k - 1$ since $d^{-1} \in D$.

Let $d \in (G \setminus D) \setminus \{e\}$. Consider $xy^{-1} = d$, where $x, y \in D$, and thus $x = dy$. Note that $y \in D \setminus \{d^{-1}\}$. Therefore, $0 \leq \mu \leq k$ since $d^{-1} \in G \setminus D \setminus \{e\}$. \square

Furthermore, if D is non-trivial, there are further restrictions on the parameters:

Proposition 1.3.4 Let D be a regular PDS with parameters $(v, k, \lambda, \mu, \beta, \Delta)$. The following statements are equivalent:

(a) D is non-trivial.

(b) $-\sqrt{\Delta} < \beta < \sqrt{\Delta} - 2$.

(c) $1 \leq \mu \leq k - 1$.

Proof:

To prove that (a) is equivalent to (b):

(Necessity) Assume that D is non-trivial. Suppose $k = \mu$. Then $\gamma = 0$ and $\Delta = \beta^2$.

By Proposition 1.3.3(b),

$$\begin{aligned} k &= \frac{(v + \beta) + \sqrt{(v + \beta)^2 - 0}}{2} \\ &= v + \beta. \end{aligned}$$

Let $D_1 = G \setminus D$. As shown above, D_1 is a $(v, k_1, \lambda_1, \mu_1)$ -PDS where

$$\begin{aligned} \mu_1 &= v - 2k + \lambda = 0, \\ \lambda_1 - \mu_1 &= v - 2k + \mu = -\beta, \\ k_1 - \lambda_1 &= k - \mu = 0. \end{aligned}$$

Therefore by Theorem 1.3.1,

$$\begin{aligned}\overline{D_1 D_1^{(-1)}} &= \mu_1 \overline{G} + (\lambda_1 - \mu_1) \overline{D_1} + (k_1 - \lambda_1) e \\ &= -\beta \overline{D_1}.\end{aligned}$$

This implies that for any $x, y \in D_1$, $xy^{-1} \in D_1$. Therefore $D_1 = (G \setminus D) \cup \{e\}$ is a subgroup of G , a contradiction by Definition 1.2.4, where a subset D_1 is trivial if it is a subgroup. Thus $k \neq \mu$. By Proposition 1.3.3(d), $\gamma = k - \mu > 0$. Thus, $\frac{\Delta - \beta^2}{4} = \gamma > 0$, so

$$-\sqrt{\Delta} < \beta < \sqrt{\Delta}. \quad (1.4)$$

Suppose $\lambda = k - 1$. From the proof of Proposition 1.3.3(a), we have $k^2 = \mu v + (\lambda - \mu)k + \gamma$, which gives $\mu(v - k - 1) = 0$. Since D is non-trivial, $v \neq k - 1$ and $\mu \leq 0$, so that there is a contradiction. Thus $\lambda \neq k - 1$. By Proposition 1.3.3(d), this implies that $\gamma = k - \mu = k - \lambda + \beta > 1 + \beta$. This also implies that $\frac{\Delta - \beta^2}{4} > \beta + 1$, so

$$-\sqrt{\Delta} - 2 < \beta < \sqrt{\Delta} - 2. \quad (1.5)$$

Consider both (1.4) and (1.5), and we have $-\sqrt{\Delta} < \beta < \sqrt{\Delta} - 2$.

(Sufficiency) Assume that D is trivial. If $D \cup \{e\}$ is a subgroup of G , then as previously stated, $\beta + 2 = \sqrt{\Delta}$. If $(G \setminus D)$ is a subgroup of G , then again as previously stated, $\beta = \sqrt{\Delta}$. Therefore, we do not have $-\sqrt{\Delta} < \beta < \sqrt{\Delta} - 2$.

Next, we prove (a) is equivalent to (c).

(Necessity) As previously stated, if D is non-trivial, then $0 \leq \mu \leq k - 1$. If $\mu = 0$, $D \cup \{e\}$ is a subgroup of G , a contradiction. Thus, $1 \leq \mu \leq k - 1$.

(Sufficiency) Assume that D is trivial. If $D \cup \{e\}$ is a subgroup of G , then $\mu = 0$. However, if $(G \setminus D)$ is a subgroup of G , then $\mu = v - (v - k) = k$. Therefore, we do not have $1 \leq \mu \leq k - 1$.

Character Values and Duals of PDS

2.1 Abelian Characters

Let G be a finite abelian group.

Definition 2.1.1 A *character* χ of G is a homomorphism from G into the multiplicative group of complex roots of unity.

The image of an element g in G under χ is written as $\chi(g)$. If the exponent of G is n , then $\chi(g)$ must be an n -th root of unity. Let G^* denote the character group of G , where the multiplication of $\chi_1, \chi_2 \in G^*$, is defined to be the character $\chi_1\chi_2$ such that $\chi_1\chi_2(g) = \chi_1(g)\chi_2(g)$. It is known that $|G^*| = |G|$ and for all $g \in G$, G^* is also isomorphic to G , see K.Ireland and M.Rosen, 1982. [7].

Definition 2.1.2 The *principle character* is defined to be the identity of the character group.

Let χ_0 denote the principle character. Note that χ_0 maps every element of G to 1.

Definition 2.1.3 The characters of G can be extended linearly to mapping from the group ring $\mathbb{C}[G]$ to \mathbb{C} . Let $\chi \in G^*$, $A \in \mathbb{C}[G]$, where $A = \sum_{g \in G} a_g g$ and $a_g \in \mathbb{C}$.

Define $\chi(A) = \sum_{g \in G} a_g \chi(g)$.

Let $A, B \in \mathbb{C}[G]$ and $c \in \mathbb{C}$, it is easy to check that

$$\chi(A + B) = \chi(A) + \chi(B)$$

$$\chi(AB) = \chi(A)\chi(B)$$

$$\chi(cA) = c\chi(A)$$

Thus, from the above we can see that χ can be regarded as a homomorphism from $\mathbb{C}[G]$ to \mathbb{C} .

Proposition 2.1.1

$$(a) \sum_{g \in G} \chi(g) = \begin{cases} |G|, & \text{if } \chi = \chi_0, \\ 0, & \text{if } \chi \neq \chi_0, \end{cases}$$

$$(b) \sum_{\chi \in G^*} \chi(g) = \begin{cases} |G|, & \text{if } g = e, \\ 0, & \text{if } g \neq e. \end{cases}$$

Proof:

Clearly, $\sum_{g \in G} \chi_0(g) = \sum_{g \in G} 1 = |G|$. If $\chi \neq \chi_0$, then there exists $b \in G$ such that $\chi(b) \neq 1$. Then,

$$\begin{aligned} \chi(b) \sum_{g \in G} \chi(g) &= \sum_{g \in G} \chi(b)\chi(g) \\ &= \sum_{g \in G} \chi(bg) \\ &= \sum_{g \in G} \chi(g) \end{aligned}$$

Since $\chi(b) \neq 1$, we have $\sum_{g \in G} \chi(g) = 0$. This proves (a). Similarly, (b) can be proven in the same way.

2.2 Fourier Inversion Formula

Theorem 2.2.1 Let $A = \sum_{g \in G} a_g g \in \mathbb{C}[G]$, where $a_g \in \mathbb{C}$.

Then for every $g \in G$,

$$a_g = \frac{1}{|G|} \sum_{\chi \in G^*} \chi(A) \chi(g^{-1}).$$

Proof:

Observe that

$$\begin{aligned} \frac{1}{|G|} \sum_{\chi \in G^*} \chi(A) \chi(g^{-1}) &= \frac{1}{|G|} \sum_{\chi \in G^*} \sum_{h \in G} a_h \chi(h) \chi(g^{-1}) \\ &= \frac{1}{|G|} \sum_{h \in G} a_h \sum_{\chi \in G^*} \chi(hg^{-1}) \end{aligned}$$

We first compute $\sum_{\chi \in G^*} \chi(hg^{-1})$.

Case 1: $h = g$

$$\sum_{\chi \in G^*} \chi(hg^{-1}) = \sum_{\chi \in G^*} \chi(1) = \sum_{\chi \in G^*} 1 = |G^*| = |G|$$

Case 2: $h \neq g$

Let $\alpha = hg^{-1} \neq 1$, and χ_1 be a character of G^* such that $\chi_1(\alpha) \neq 1$.

Then

$$\chi_1(\alpha) \sum_{\chi \in G^*} \chi(\alpha) = \sum_{\chi \in G^*} (\chi_1 \chi)(\alpha) = \sum_{\chi \in G^*} \chi(\alpha)$$

Therefore,

$$\begin{aligned} (1 - \chi_1(\alpha)) \sum_{\chi \in G^*} \chi(\alpha) &= 0 \\ \implies \sum_{\chi \in G^*} \chi(\alpha) &= 0 \quad \text{because } \chi_1(\alpha) \neq 1. \end{aligned}$$

Thus,

$$\begin{aligned} \frac{1}{|G|} \sum_{\chi \in G^*} \chi(A) \chi(g^{-1}) &= \frac{1}{|G|} \sum_{h \in G} a_h \sum_{\chi \in G^*} \chi(hg^{-1}) \\ &= \frac{1}{|G|} |G| a_g \\ &= a_g \quad \square \end{aligned}$$

Corollary 2.2.1 Let y and z be elements of $\mathbb{C}[G]$. Then $y = z$ if and only if $\chi(y) = \chi(z)$, for all $\chi \in G^*$.

Proof:

For necessity, just apply the function χ on both sides.

For sufficiency, suppose $\chi(y) = \chi(z)$ for all $\chi \in G^*$ where $y = \sum_{g \in G} a_g g$ and $z = \sum_{g \in G} b_g g$. Then by Theorem 2.3.1,

$$\begin{aligned} a_g &= \frac{1}{|G|} \sum_{\chi \in G^*} \chi(y) \chi(g^{-1}) \\ &= \frac{1}{|G|} \sum_{\chi \in G^*} \chi(z) \chi(g^{-1}) \\ &= b_g \end{aligned} \tag{2.1}$$

for all $g \in G$. Therefore, $y = z$. \square

In the following, we introduce the Finite Fourier Transform, which is an important tool in the study of PDS.

Definition 2.2.1 Let $A = \sum_{g \in G} a_g g \in \mathbb{C}[G]$. Then the Finite Fourier Transform of A is given by

$$\widehat{A} = \sum_{\chi \in G^*} (\chi(A)) \chi.$$

From definition, it can be seen that $\widehat{A} \in \mathbb{C}[G^*]$.

Let $A = \sum_{g \in G} a_g g$ and $B = \sum_{g \in G} b_g g$. Under Finite Fourier Transform, we can see that $\widehat{A+B} = \widehat{A} + \widehat{B}$, $\widehat{AB} = \widehat{A} * \widehat{B}$ and also $\widehat{A * B} = \frac{1}{|G|} \widehat{AB}$, where the operation $*$ is defined as $A * B = \sum_{g \in G} (a_g b_g) g$.

If σ is the canonical isomorphism from G to $(G^*)^*$, i.e. $\sigma(g) = X_g$ where $X_g(\chi) = \chi(g)$ for all $\chi \in G^*$, then we have the following result:

Proposition 2.2.1 Let $A = \sum_{g \in G} a_g g \in \mathbb{C}[G]$. Then $\sigma^{-1}(\widehat{A}) = |G| \sum_{g \in G} a_g g^{-1}$.

Proof:

$$\begin{aligned}
\widehat{A} &= \sum_{X_g \in (G^*)^*} (X_g(\widehat{A}))X_g \\
&= \sum_{g \in G} (X_g(\widehat{A}))X_g \\
&= \sum_{g \in G} \left[X_g \left(\sum_{\chi \in G^*} (\chi(A))\chi \right) \right] X_g \\
&= \sum_{g \in G} \left[\sum_{\chi \in G^*} \chi(A)\chi(g) \right] X_g \\
&= \sum_{g \in G} \left[\sum_{\chi \in G^*} \chi(A)\chi(g^{-1}) \right] X_{g^{-1}} \\
&= \sum_{g \in G} |G|a_g X_{g^{-1}}
\end{aligned}$$

by Theorem 2.2.1. Hence,

$$\begin{aligned}
\sigma^{-1}(\widehat{A}) &= \sum_{g \in G} |G|a_g \sigma^{-1}(X_{g^{-1}}) \\
&= \sum_{g \in G} |G|a_g g^{-1}. \quad \square
\end{aligned}$$

2.3 Character Values of PDS

This section will illustrate how character values can enable us to detect PDS.

Proposition 2.3.1 Let G be an abelian group of order v and D be a subset of G such that $D^{(-1)} = D$. Then D is a (v, k, λ, μ) -PDS in G and $\chi \in G^*$, if and only if

$$\chi \overline{D} = \begin{cases} k & \text{if } \chi \text{ is trivial,} \\ \frac{\beta \pm \sqrt{\Delta}}{2} & \text{if } \chi \text{ is not trivial,} \end{cases} \quad (2.2)$$

where $\gamma = k - \mu$ if $e \notin D$ and $\gamma = k - \lambda$ if $e \in D$, $\beta = \lambda - \mu$ and $\Delta = \beta^2 + 4\gamma$.

Proof:

(Necessity)

Assume that D is a (v, k, λ, μ) -PDS in G . If χ is trivial, then clearly, by Proposition 2.1.1, $\chi\bar{D} = k$. If χ is non-trivial, then by applying χ to (1.3), we have a quadratic equation in $\chi\bar{D}$:

$$\begin{aligned}(2\bar{D} - \beta e)^2 &= 4\mu\bar{G} + \Delta e \\ \chi((2\bar{D} - \beta e)^2) &= \chi(4\mu\bar{G} + \Delta e) \\ 4(\chi\bar{D})^2 - 4\beta(\chi\bar{D}) + \beta^2 &= 0 + \Delta\end{aligned}$$

Therefore, the above quadratic equation in $\chi\bar{D}$ can be solved to obtain $\chi\bar{D} = \frac{\beta \pm \sqrt{\Delta}}{2}$.

(Sufficiency)

Case 1: χ is trivial.

Assume that $\chi\bar{D} = k$. From (1.2), we have $k^2 = \mu v + (\lambda - \mu)k + \gamma$. Therefore, by Corollary 2.3.1,

$$\begin{aligned}(\chi\bar{D})^2 &= k^2 = \mu v + (\lambda - \mu)k + \gamma \\ (\chi\bar{D})^2 &= \mu\chi\bar{G} + (\lambda - \mu)\chi\bar{D} + \gamma\chi(e) \\ \bar{D}^2 &= \mu\bar{G} + (\lambda - \mu)\bar{D} + \gamma e\end{aligned}$$

By Theorem 1.3.1, D is a (v, k, λ, μ) -PDS in G .

Case 2: χ is non-trivial.

Assume that $\chi\bar{D} = \frac{\beta \pm \sqrt{\Delta}}{2}$, we work the second part of the necessity proof backwards to obtain our result:

$$\begin{aligned}\chi\bar{D} &= \frac{\beta \pm \sqrt{\Delta}}{2} \\ 2\chi\bar{D} - \beta &= \pm\sqrt{\Delta} \\ (2\chi\bar{D} - \beta)^2 &= \Delta \\ \chi((2\bar{D} - \beta e)^2) &= \chi(4\mu\bar{G} + \Delta e) && \text{(by Proposition 2.1.1 (a))} \\ (2\bar{D} - \beta e)^2 &= 4\mu\bar{G} + \Delta e && \text{(by Corollary 2.3.1)}\end{aligned}$$

By Theorem 1.3.1, D is a (v, k, λ, μ) -PDS in G . \square

Definition 2.3.1 Let G be an abelian group of order v and D be a (v, k, λ, μ) -PDS in G with $D^{(-1)} = D$. If $D \neq \emptyset$, $\{e\}$, $G \setminus \{e\}$ and G , then the *dual* of D is defined to be $D^+ = \{\chi \in G^* : \chi \text{ is non-trivial and } \chi \bar{D} = (\beta + \sqrt{\Delta})/2\}$. Note that if $e \in D$, then $D^+ = (D \setminus \{e\})^+$.

Then the dual D^+ of D is a regular PDS in G^* with parameters as follows:

$$(v^+, k^+, \lambda^+, \mu^+, \beta^+, \Delta^+) = (v, [(\sqrt{\Delta} - \beta)(v - 1) - 2k]/(2\sqrt{\Delta}), \beta^+ + \mu^+, [4k^+ - \Delta^+ + (\beta^+)^2]/4, (v - 2k + \beta - \sqrt{\Delta})/\sqrt{\Delta}, v^2/\Delta).$$

Proof:

By Proposition 2.3.1, the Finite Fourier Transform of \bar{D} is given by

$$\begin{aligned} \widehat{\bar{D}} &= \frac{\beta + \sqrt{\Delta}}{2} \bar{D}^+ + \frac{\beta - \sqrt{\Delta}}{2} \overline{(G^* \setminus D^+) \setminus \{\chi_0\}} + k\chi_0 \\ &= \frac{\beta - \sqrt{\Delta}}{2} \bar{G}^* + \sqrt{\Delta} \bar{D}^+ + \left(k - \frac{\beta - \sqrt{\Delta}}{2}\right) \chi_0. \end{aligned}$$

Thus, $\sqrt{\Delta} \bar{D}^+ = \widehat{\bar{D}} - \frac{\beta - \sqrt{\Delta}}{2} \bar{G}^* + \left(\frac{\beta - \sqrt{\Delta}}{2} - k\right) \chi_0$. Let σ be the canonical isomorphism between G and $(G^*)^*$. By taking the Finite Fourier Transform followed by applying σ^{-1} , we have

$$\begin{aligned} \sigma^{-1}(\sqrt{\Delta} \widehat{\bar{D}^+}) &= \sigma^{-1}(\widehat{\bar{D}}) - \frac{\beta - \sqrt{\Delta}}{2} \sigma^{-1}(\widehat{\bar{G}^*}) + \left(\frac{\beta - \sqrt{\Delta}}{2} - k\right) \sigma^{-1}(\widehat{\chi_0}) \\ &= \sigma^{-1}(\widehat{\bar{D}}) - \frac{\beta - \sqrt{\Delta}}{2} \sigma^{-1}(|G^*| X_e) + \left(\frac{\beta - \sqrt{\Delta}}{2} - k\right) \sigma^{-1}(\overline{(G^*)^*}) \\ &= \sigma^{-1}(\widehat{\bar{D}}) - \frac{\beta - \sqrt{\Delta}}{2} v e + \left(\frac{\beta - \sqrt{\Delta}}{2} - k\right) \bar{G} \\ &= v \bar{D} + \left(\frac{\beta - \sqrt{\Delta}}{2} - k\right) \bar{G} - \frac{\beta - \sqrt{\Delta}}{2} v e \end{aligned}$$

using Proposition 2.2.1. This implies that

$$\sqrt{\Delta} \sum_{g \in G} (X_g \bar{D}^+) g = v \bar{D} + \left(\frac{\beta - \sqrt{\Delta}}{2} - k\right) \bar{G} - \frac{\beta - \sqrt{\Delta}}{2} v e.$$

Therefore, $X_e \overline{D^+} = \frac{1}{\sqrt{\Delta}} \left(\frac{\beta - \sqrt{\Delta}}{2} - k - \frac{\beta - \sqrt{\Delta}}{2} v \right) = \frac{(\sqrt{\Delta} - \beta)(v - 1) - 2k}{2\sqrt{\Delta}}$.

If X_g is non-trivial and $g \in D$, then $X_g \overline{D^+} = \frac{1}{\sqrt{\Delta}} \left[v + \frac{\beta - \sqrt{\Delta}}{2} - k \right]$.

If X_g is non-trivial and $g \notin D$, then $X_g \overline{D^+} = \frac{1}{\sqrt{\Delta}} \left[\frac{\beta - \sqrt{\Delta}}{2} - k \right]$.

Thus, (2.2) holds with $k^+ = \frac{(\sqrt{\Delta} - \beta)(v - 1) - 2k}{2\sqrt{\Delta}}$, $\beta^+ = \frac{v - 2k + \beta - \sqrt{\Delta}}{\sqrt{\Delta}}$,

and $\Delta^+ = \frac{v^2}{\Delta}$. By Theorem 2.3.1, we find that D^+ is a PDS in G^* with parameters

$(v^+, k^+, \lambda^+, \mu^+, \beta^+, \Delta^+) =$

$$\left(v, \frac{(\sqrt{\Delta} - \beta)(v - 1) - 2k}{2\sqrt{\Delta}}, \beta^+ + \mu^+, \frac{4k^+ - \Delta^+ + (\beta^+)^2}{4}, \frac{v - 2k + \beta - \sqrt{\Delta}}{\sqrt{\Delta}}, \frac{v^2}{\Delta} \right). \quad \square$$

Remark 2.3.1 By (1.3), we have

$$\left[2\overline{D^+} - \left(\frac{v - 2k + \beta - \sqrt{\Delta}}{\sqrt{\Delta}} \right) \chi_0 \right]^2 = \frac{v}{\Delta} [(\sqrt{\Delta} - \beta - 1)^2 - 1] \overline{G^*} + \frac{v^2}{\Delta} \chi_0 \quad (2.3)$$

where χ_0 is the trivial character of G .

2.4 Some Number Theory

Throughout this section, the results would be stated without proof. These well-known results can be found in K.Ireland and M.Rosen, 1982 [7]. The results here are used in the proof of Paley PDS, to be shown in the next chapter.

Definition 2.4.1 Let q be an odd prime. For any non-zero $a \in \mathbb{F}_q$, we define the *Legendre symbol* as follows:

$$\left(\frac{a}{q} \right) = \begin{cases} 0 & \text{if } a = 0, \\ 1 & \text{if } a \text{ is a square in } \mathbb{F}_q, \\ -1 & \text{if } a \text{ is not a square in } \mathbb{F}_q. \end{cases}$$

Definition 2.4.2 Let q be an odd prime and $\zeta_q = e^{\frac{2\pi i}{q}}$. For any integer r such that $0 \leq r \leq q - 1$, we define the *Gauss sum* as follows:

$$G_q(r) = \sum_{a=1}^{q-1} \left(\frac{a}{q}\right) \zeta_q^{ra}.$$

Theorem 2.4.1

(a) $G_q(r) = \left(\frac{r}{q}\right) G_q(1)$ for $1 \leq r \leq q - 1$;

(b) $[G_q(1)]^2 = \left(\frac{-1}{q}\right)q$.

Theorem 2.4.2 Let q be an odd prime, $q^* = \left(\frac{-1}{q}\right)q$ and $\zeta_q = e^{\frac{2\pi i}{q}}$. If $D = \left\{a \in \mathbb{F}_q \setminus \{0\} : \left(\frac{a}{q}\right) = 1\right\}$, then $\sum_{a \in D} \zeta_q^a = \frac{\sqrt{q^*}-1}{2}$.

Examples of Regular PDS

3.1 Paley PDS

This is obtained from K.M. Ng. 1994. [4]

Theorem 3.1.1 Let G be the additive group of a finite field \mathbb{F}_q where q is an odd prime power and $q \equiv 1 \pmod{4}$. Then the set D of all nonzero squares in \mathbb{F}_q forms a regular $(q, (q - 1)/2, (q - 5)/4, (q - 1)/4)$ -PDS in G . Note that $\beta = -1$ and $\Delta = q$.

Proof:

Case 1:

Let χ be a non-trivial element of G^* . Then $\chi(1) = \zeta_q^r$ for some $r \nmid q$, where $\zeta_q = e^{\frac{2\pi i}{q}}$.

Hence $\chi(a) = \zeta_q^{ra}$ for $a = 1, 2, \dots, q - 1$. We have

$$\begin{aligned}
 1 + \sum_{a=1}^{q-1} \chi(a) &= \sum_{a=0}^{q-1} \zeta_q^{ra} \\
 &= \frac{\zeta_q^{rq} - 1}{\zeta_q^r - 1} \\
 &= 0.
 \end{aligned} \tag{3.1}$$

Let $D_1 = (G \setminus D) \setminus \{0\}$. From Theorem 2.4.1, $G_q(r) = \pm\sqrt{q}$. By definition, we also have

$G_q(r) = \sum_{a=1}^{q-1} \left(\frac{a}{q}\right) \chi(a) = \sum_{a \in D} \chi(a) - \sum_{a \in D_1} \chi(a)$. Therefore,

$$\sum_{a \in D} \chi(a) - \sum_{a \in D_1} \chi(a) = \pm\sqrt{q}. \tag{3.2}$$

By (3.1) and (3.2), $\frac{1}{2} + \sum_{a \in D} \chi(a) = \pm \frac{\sqrt{q}}{2}$, so that $\chi \bar{D} = \frac{-1 \pm \sqrt{q}}{2}$.

By Theorem 2.3.1, D is a regular $(q, (q-1)/2, (q-5)/4, (q-1)/4)$ -PDS in G , with $\beta = -1$ and $\Delta = q$.

Case 2:

If χ is trivial, $\chi \bar{D} = \frac{q-1}{2}$. Then (2.2) holds with $k = \frac{q-1}{2}$, $\beta = -1$, and $\Delta = q$.

Since $0 \notin D$, by Theorem 2.3.1, D is a (v, k, λ, μ) -PDS where $v = q$, $k = \frac{q-1}{2}$, $\mu = k - \frac{\Delta - \beta^2}{4} = \frac{q-1}{4}$, and $\lambda = \beta + \mu = \frac{q-5}{4}$. \square

Definition 3.1.1 A PDS is called a Paley PDS if it has the parameters $(v, k, \lambda, \mu) = (v, (v-1)/2, (v-5)/4, (v-1)/4)$.

Example 3.1.1 The PDS with parameters $(5, 2, 0, 1, -1, 5)$ is a Paley PDS.

3.2 PCP

Let G be a group of order n^2 . A partial congruence partition of G with degree r (an (n, r) -PCP) is a set \mathcal{P} of r subgroups of G of order n such that $U \cap V = \{e\}$ for every pair of distinct elements U, V of \mathcal{P} .

This is obtained from S.L. Ma. 1994. [3]

Theorem 3.2.1 Let G be a group of order n^2 and \mathcal{P} be an (n, r) -PCP of G . Then $D = \bigcup_{U \in \mathcal{P}} (U \setminus \{e\})$ is a regular $(n^2, r(n-1), n+r^2-3r, r^2-r)$ -PDS in G . Note that $\beta = n-2r$ and $\Delta = n^2$.

Proof:

Let U_1, U_2, \dots, U_r be the r subgroups of G in \mathcal{P} . For $i \neq j$, $U_i U_j = G$ so that

$\bar{U}_i \bar{U}_j^{(-1)} = \bar{G}$, For $i = j$, $\bar{U}_i \bar{U}_j^{(-1)} = n\bar{U}_i$. Therefore,

$$\begin{aligned}
\bar{D}\bar{D}^{(-1)} &= \sum_{1 \leq i, j \leq r} (\bar{U}_i - e)(\bar{U}_j^{(-1)} - e) \\
&= \sum_{1 \leq i, j \leq r} \bar{U}_i \bar{U}_j^{(-1)} - \sum_{1 \leq i, j \leq r} \bar{U}_i - \sum_{1 \leq i, j \leq r} \bar{U}_j^{(-1)} + \sum_{1 \leq i, j \leq r} e \\
&= (r^2 - r)\bar{G} + n \sum_{1 \leq i, j \leq r} \bar{U}_i - r \sum_{1 \leq i, j \leq r} \bar{U}_i - r \sum_{1 \leq i, j \leq r} \bar{U}_j^{(-1)} + r^2 e \\
&= (r^2 - r)\bar{G} + (n - 2r) \sum_{1 \leq i, j \leq r} \bar{U}_i + r^2 e \\
&= (r^2 - r)\bar{G} + (n - 2r)\bar{D} + (rn - r^2)e.
\end{aligned}$$

Thus, D is a regular $(n^2, r(n - 1), n + r^2 - 3r, r^2 - r)$ -PDS in G by Theorem 1.3.1.

□

Example 3.2.1

1. Let $G = H \times K$ where H and K are groups of order n . Then $D = \{(h, e) : h \in H \setminus \{e\}\} \cup \{(e, g) : g \in K \setminus \{e\}\}$ is a regular $(n^2, 2(n - 1), n - 2, 2)$ -PDS in G .
2. Let $G = H \times H$ where H is a group of order n . Then $D = \{(h, e), (e, h), (h, h) : h \in H \setminus \{e\}\}$ is a regular $(n^2, 3(n - 1), n, 6)$ -PDS in G .
3. Let G be the additive group of a vector space of dimension 2 over a finite field \mathbb{F}_q and H_1, H_2, \dots, H_r (where $r \leq q + 1$) be r distinct hyperplanes of the vector space. Then $D = (H_1 \cup H_2 \cup \dots \cup H_r) \setminus \{0\}$ is a regular $(q^2, r(q - 1), q + r^2 - 3r, r^2 - r)$ -PDS in G .

The following theorem gives some conditions regarding the existence of PCPs in an abelian group G of order n^2 and will be stated without proof.

Theorem 3.2.2 This is obtained from R.A. Bailey and D. Jungnickel, 1990.[8]

Let G be an abelian group of order n^2 with $n = p_1^{a_1} p_2^{a_2} \dots p_s^{a_s}$ where p_1, p_2, \dots, p_s are distinct primes.

- (a) If $r > \min\{p_i^{a_i} + 1\}$, then no (n, r) -PCP exists in G .
- (b) Suppose all Sylow p_i -subgroups of G are elementary abelian. Then an (n, r) -PCP exists in G if and only if $1 \leq r \leq \min\{p_i^{a_i} + 1\}$.

Corollary 3.2.1 Let $n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$ where p_1, p_2, \dots, p_s are distinct primes. Then there exists an abelian regular $(n^2, r(n - 1), n + r^2 - 3r, r^2 - r)$ -PDS whenever $1 \leq r \leq \min\{p_i^{a_i} + 1\}$.

Please refer to the Appendix for more examples.

Table of Parameters

4.1 Conditions

In this section, we give a list of conditions and restrictions on the parameters $(v, k, \lambda, \mu, \beta, \Delta)$ with $v < 200$, as shown in the table 4.2.

First, we obtain a list of possible values of v, k, λ , and μ with

$$5 \leq v \leq 200, 2 \leq k \leq 200, 0 \leq \lambda \leq k - 1 \text{ and } 1 \leq \mu \leq k - 1. \quad (4.1)$$

Other parameters are calculated by the formulae

$$\beta = \lambda - \mu, \Delta = \beta^2 + 4(k - \mu) \text{ and } v = (k^2 - \beta k - k + \mu)/\mu. \quad (4.2)$$

Then the parameters obtained are tested with the following criterions, (i), (ii) and (iii) drawn from Proposition 1.3.3, the rest from S.L. Ma, 1994. [3]:

- (i) β and Δ has the same parity;
- (ii) $v^2 \equiv (2k - \beta)^2 \equiv (\beta^2 + 2\beta)v \equiv 0 \pmod{\Delta}$;
- (iii) $v, \Delta, v^2/\Delta$ have the same prime divisors;
- (iv) if Δ is not a square, then there exists an odd prime $p \equiv 1 \pmod{4}$ such that $(v, k, \lambda, \mu, \beta, \Delta) = (p^{2s+1}, (p^{2s+1} - 1)/2, (p^{2s+1} - 5)/4, (p^{2s+1} - 1)/4, -1, p^{2s+1})$; and

(v) if $v = p^s$, where p is a prime, and Δ is a square, then k is a multiple of $p - 1$.

If D is a nontrivial abelian regular PDS with parameters $(v, k, \lambda, \mu, \beta, \Delta)$, then $D' = (G \setminus D) \setminus \{e\}$ is a regular PDS with parameters

$$(v', k', \lambda', \mu', \beta', \Delta') = (v, v - k - 1, v - 2k - 2 + \mu, v - 2k + \lambda, -\lambda - 2, \Delta)$$

and the dual D^+ is a regular PDS with parameters

$$(v^+, k^+, \lambda^+, \mu^+, \beta^+, \Delta^+) = (v, [(\sqrt{\Delta} - \beta)(v - 1) - 2k]/(2\sqrt{\Delta}), \beta^+ + \mu^+, [4k^+ - \Delta^+ + (\beta^+)^2]/4, (v - 2k + \beta - \sqrt{\Delta})/\sqrt{\Delta}, v^2/\Delta).$$

Hence we only list those parameters with $k \leq (v - 1)/2$ and $\Delta \leq v$, since the case $k > (v - 1)/2$ can be obtained by the complement, and the case $\Delta > v$ can be obtained by the dual.

Theorem 4.1.1 Suppose there exists a nontrivial regular (v, k, λ, μ) -PDS in an abelian group where v is not a prime power. Let p be an odd prime divisor of v , say $v = p^t u$ and $\Delta = p^{2r} \pi^2$ where $p \nmid u$ and $p \nmid \pi$. Let $\beta_1 = \beta - 2\theta\pi$ where $(2\theta - 1)\pi \leq \beta < (2\theta + 1)\pi$. Then

(a) $A = (u + \beta_1)^2 - (\pi^2 - \beta_1^2)(u - 1)$ is a square; and

(b) either $k_1 = (u + \beta_1 - \sqrt{A})/2$ or $k_1 = (u + \beta_1 + \sqrt{A})/2$ satisfies all of the following:

(i) $0 \leq k_1 < \min\{k, u\}$;

(ii) if $k_1 \neq 0$ and $u - 1$ then $\lambda_1, \mu_1, u - 2k_1 + \lambda_1, u - 2k_1 - 2 + \mu_1$ are non-negative where $u_1 = k_1 - [(\pi^2 - \beta_1^2)/4]$ and $\lambda_1 = \beta_1 + \mu_1$; and

(iii) if $p \geq 5$ and $k_1 \neq 0, u - 1$, then either (1) r is even and $\theta \equiv 0 \pmod{p - 1}$ or (2) r is odd and $\theta \equiv (p - 1)/2 \pmod{p - 1}$.

The Table 4.2 gives a table of parameters satisfying the conditions listed above. In the following, *Paley* refers to regular PDSs constructed by Theorem 3.1.1; *PCP* refers to

regular PDSs constructed by Theorem 3.2.1; others: examples A.1.1, A.1.2, A.1.3, A.1.4 and A.1.5 are listed by specific examples in the Appendix A.1, non-existence theorems A.2.1 and A.2.2 are found in Appendix A.2; and ??? means the existence of such a regular PDS is still unknown.

4.2 Table of Parameters

No.	v	k	λ	μ	β	Δ	Examples/Remark
1	5	2	0	1	-1	5	Paley
2	9	4	1	2	-1	9	(3, 2)PCP
3	13	6	2	3	-1	13	Paley
4	16	5	0	2	-2	16	Example A.1.1
5	16	6	2	2	0	16	(4, 2)PCP
6	17	8	3	4	-1	17	Paley
7	25	8	3	2	1	25	(5, 2)PCP
8	25	12	5	6	-1	25	(5, 3)PCP
9	29	14	6	7	-1	29	Paley
10	36	10	4	2	2	36	(6, 2)PCP
11	36	14	4	6	-2	36	Example A.1.4
12	36	15	6	6	0	36	(6, 3)PCP
13	37	18	8	9	-1	37	Paley
14	41	20	9	10	-1	41	Paley
15	49	12	5	2	3	49	(7, 2)PCP
16	49	18	7	6	1	49	(7, 3)PCP
17	49	24	11	12	-1	49	(7, 4)PCP
18	53	26	12	13	-1	53	Paley
19	61	30	14	15	-1	61	Paley
20	64	14	6	2	4	64	(8, 2)PCP
21	64	18	2	6	-4	64	Example A.1.2
22	64	21	8	6	2	64	(8, 3)PCP
23	64	27	10	12	-2	64	Example A.1.4
24	64	28	12	12	0	64	(8, 4)PCP
25	73	36	17	18	-1	73	Paley
26	81	16	7	2	5	81	(9, 2)PCP
27	81	20	1	6	-5	81	Example A.1.5 (2)

No.	v	k	λ	μ	β	Δ	Examples/Remark
28	81	24	9	6	3	81	(9, 3)PCP
29	81	30	9	12	-3	81	Example A.1.3
30	81	32	13	12	1	81	(9, 4)PCP
31	81	40	19	20	-1	81	(9, 5)PCP
32	89	44	21	22	-1	89	Paley
33	97	48	23	24	-1	97	Paley
34	100	18	8	2	6	100	(10, 2)PCP
35	100	22	0	6	-6	100	NOT EXIST by theorem A.2.2
36	100	27	10	6	4	100	(10, 3)PCP
37	100	33	8	12	-4	100	???
38	100	36	14	12	2	100	???
39	100	44	18	20	-2	100	NOT EXIST by theorem A.2.1
40	100	45	20	20	0	100	NOT EXIST by theorem A.2.1
41	101	50	24	25	-1	101	Paley
42	109	54	26	27	-1	109	Paley
43	113	56	27	28	-1	113	Paley
44	121	20	9	2	7	121	(11, 2)PCP
45	121	30	11	6	5	121	(11, 3)PCP
46	121	40	15	12	3	121	(11, 4)PCP
47	121	50	21	20	1	121	(11, 5)PCP
48	121	60	29	30	-1	121	(11, 6)PCP
49	125	62	30	31	-1	125	Paley
50	137	68	33	34	-1	137	Paley
51	144	22	10	2	8	144	(12, 2)PCP
52	144	33	12	6	6	144	(12, 3)PCP
53	144	39	6	12	-6	144	???
54	144	44	16	12	4	144	(12, 4)PCP

No.	v	k	λ	μ	β	Δ	Examples/Remark
55	144	52	16	20	-4	144	???
56	144	55	22	20	2	144	???
57	144	65	28	30	-2	144	Example A.1.4
58	144	66	30	30	0	144	Example A.1.4
59	149	74	36	37	-1	149	Paley
60	157	78	38	39	-1	157	Paley
61	169	24	11	2	9	169	(13, 2)PCP
62	169	36	13	6	7	169	(13, 3)PCP
63	169	48	17	12	5	169	(13, 4)PCP
64	169	60	23	20	3	169	(13, 5)PCP
65	169	72	31	30	1	169	(13, 6)PCP
66	169	84	41	42	-1	169	(13, 7)PCP
67	173	86	42	43	-1	173	Paley
68	181	90	44	45	-1	181	Paley
69	193	96	47	48	-1	193	Paley
70	196	26	12	2	10	196	(14, 2)PCP
71	196	39	14	6	8	196	(14, 3)PCP
72	196	45	4	12	-8	196	NOT EXIST by theorem A.2.2
73	196	52	18	12	6	196	NOT EXIST by theorem A.2.2
74	196	60	14	20	-6	196	???
75	196	65	24	20	4	196	???
76	196	75	26	30	-4	196	???
77	196	78	32	30	2	196	???
78	196	90	40	42	-2	196	NOT EXIST by theorem A.2.1
79	196	91	42	42	0	196	NOT EXIST by theorem A.2.1
80	197	98	48	49	-1	197	Paley

Examples of PDS

A.1 Examples

We list the examples used in the table 4.2 which were not shown in Chapter 3.

Please refer to S.L. Ma, 1994. [3]

Example A.1.1 Let $C = \{00000, 11111\}$ be a binary repetition code. Then C^\perp is generated by 1000, 1100, 0110, 0011, 0001 over \mathbb{F}_2 . The PDS corresponding to C^\perp has parameters $(v, k, \lambda, \mu) = (16, 5, 0, 2)$.

Example A.1.2 Let \mathcal{O} be a hyperoval in $PG(2, 2^m)$, i.e., \mathcal{O} is a set of $n = 2^m + 2$ points, no three collinear, and with the property that $|L \cap \mathcal{O}| = 0$ or 2 for any line L in $PG(2, 2^m)$. There are three unique examples when $m = 1, 2$ and 3 but many different examples for larger m . The code over \mathbb{F}_2^m obtained from \mathcal{O} is a two-weight $(2^m + 2, 3)$ -projective code with nonzero weights 2^m and $2^m + 2$. The corresponding regular PDS has parameters $(v, k, \lambda, \mu, \beta, \Delta) = (2^{3m}, (2^m + 2)(2^m - 1), (2^m - 2), 2^m + 2, -4, 2^{2m+2})$.

Example A.1.3 $D = C_0 \cup C_1 \cup C_3$, where the C_i are the 8th cyclotomic classes in \mathbb{F}_3^4 , is a $(81, 30, 9, 12)$ -PDS.

Example A.1.4 Reversible $(4u^2, 2u^2 - u, u^2 - u)$ -difference sets are constructed in

abelian groups

$$G = \mathbb{Z}_2^{2a} \times \mathbb{Z}_4^b \times \left(\mathbb{Z}_{2^{q_1}}^{2c_1} \times \cdots \times \mathbb{Z}_{2^{q_s}}^{2c_s} \right) \times \mathbb{Z}_3^{2d} \times \left(\mathbb{Z}_{p_1}^{4\alpha_1} \times \cdots \times \mathbb{Z}_{p_t}^{4\alpha_t} \right)$$

with $u = \pm 2^{a+b+c_1+\cdots+c_s-1} \cdot 3^d \cdot p_1^{2\alpha_1} \cdots p_t^{2\alpha_t}$, where p_i are odd primes, see D.Jungnickel et al, 1999 [9]; $a, b, c_i, d, \alpha_i, s, t$ are nonnegative integers; and if $d + \alpha_1 + \cdots + \alpha_t > 0$, then $a > 0$. Let D be such a reversible difference set. It can be checked that there exists elements x and y in G such that $2x = 2y = 0$ and $x \in D$ while $y \notin D$. Hence $D + y$ is an abelian regular $(4u^2, 2u^2 - u, u^2 - u, u^2 - u)$ -PDS in G and $(D + x) \setminus \{0\}$ is an abelian regular $(4u^2, 2u^2 - u - 1, u^2 - u - 2, u^2 - u)$ -PDS. Note that $(4u^2, 2u^2 - u, u^2 - u, u^2 - u)$ -PDS belongs to the Latin square type if $u > 0$ and belongs to the negative Latin square type if $u < 0$.

Theorem A.1.1 Let $Q : \mathbb{F}_q^{2m} \rightarrow \mathbb{F}_q$ be a nondegenerate quadratic form. Then $D = \{x \in \mathbb{F}_q^{2m} \setminus \{0\} : Q(x) = 0\}$ is a regular $(q^{2m}, q^{2m-1} + \epsilon q^{m-1}(q-1) - 1, q^{2m-2} + \epsilon q^{m-1}(q-1) - 2, q^{2m-2} + \epsilon q^{m-1})$ -PDS in the additive group of \mathbb{F}_q^{2m} , where $\epsilon = \pm 1$ and depends on the choice of Q . Note that $\beta = \epsilon q^{m-1}(q-2) - 2$ and $\Delta = q^{2m}$.

Example A.1.5

1. When $\epsilon = 1$, the PDS constructed by Theorem A.1.1 have parameters $(v, k, \lambda, \mu) = (q^{2m}, r(q^m - 1), q^m + r^2 - 3r, r^2 - r)$, where $r = q^{m-1} + 1$, which belong to the Latin square type PDS.
2. When $\epsilon = -1$, the PDS constructed by Theorem A.1.1 have parameters $(v, k, \lambda, \mu) = (q^{2m}, r(q^m + 1), -q^m + r^2 + 3r, r^2 + r)$, where $r = q^{m-1} - 1$, which belong to the negative Latin square type PDS.

A.2 Some more non-existence theorems

The following is a restriction on the parameters of an abelian reversible Menon difference set.

Theorem A.2.1 If the square free part of u is not equal to $\pm 2^a 3^b$, then no reversible $(4u^2, 2u^2 - u, u^2 - u)$ -difference set exists in any abelian group of order $4u^2$.

For the following theorem, please refer to S.L. Ma, 1997. [6].

Theorem A.2.2 Suppose there exists a nontrivial regular (v, k, λ, μ) -PDS in an abelian group. If $2^m \parallel v$, then

$$k \leq \mu(2^m - 1) + \xi_2,$$

where

$$\xi_2 = \begin{cases} 0 & \text{if } \beta < -2, \\ \frac{(\beta+2)^2}{4} & \text{if } -2 \leq \beta < 2^{m+1} - 4, \\ (\beta - 2^m + 3)(2^m - 1) & \text{if } \beta \geq 2^{m+1} - 4. \end{cases}$$

Therefore, the PDS with parameters not fulfilling the above are non-existent.

Appendix B

C Program

```
/******  
A Table of parameters for partial difference sets in Abelian Groups  
******/  
  
#include <stdio.h>  
#include <math.h>  
#define MAX 400  
  
void find_para(int array[][6]);  
int conditions(int b, int d, int v, int k);  
int comp_prime(int A, int B, int C);  
int conditions2(int v, int k, int l, int m, int b, int d);  
int dual_compl(int v, int k, int d);  
void find_eg(int v, int k, int l, int m, int b, int d);  
int factorise(int root);  
int t15_1(int v, int k, int l, int m, int b, int d);  
int t2_2(int v, int k, int l, int m, int b, int d);  
  
/*The above are the functions used in the program  
1.find_para is the function used to find the correct parameters with the  
conditions checked.  
2.conditions function checks the conditions i), ii), iii),  
conditions2 function checks the conditions iv) and v).  
3.conditions and conditions2 are the functions where parameters are tested.  
4.comp_prime is called in conditions function to compare primes  
5.dual_compl is called to check whether it is a dual, complement or neither  
6.find_eg is called in find_para to find out what kind of example each set  
of parameters is.  
7.factorise function is used to factorise root such that  
root= P1^A1...Ps^As, and returns the minimum value (Pi^Ai + 1).
```

8.checks whether parameters are not existent under Theorem 4.1.1*/

```

int arrayp[100], arrayp_mod4[100], counter, counter1, j=0, limit;
/*above are global variables to be used throughout program.*/

main ()
{
    int array[MAX][6], i, h, flag;
    printf("Please enter limit:");
    scanf("%d", &limit); limit++;
    for (i=2, counter=0; i<limit; i++)
    {
        flag = 0;
        for (h=2; h<=i-1; h++)
            if ((i % h) == 0)
                { flag = 1; break;}
        if (flag == 0)
            { arrayp[counter]= i; counter++;};
    };

    for (i=0, counter1=0; i<counter; i++)
        if ((arrayp[i] % 4) == 1)
            { arrayp_mod4[counter1] = arrayp[i];
              counter1++; };

    /* The above two for loops generate the primes, primes % 4 == 1 within
       a range. */

    find_para(array);
}

void find_para(int array[][6])
{
    int v, k, l, m, b, d;
    int cases;
    char names[3][4] = {"reg", "dual", "comp"};
    printf("v k l m b d Example\n");
    for (v=5; v<limit; v++)
    {
        for (d=2; d<limit; d++)
        {
            if (d>v) break;
            for (k=2; k<limit; k++)
            {

```

```

    for (n=0; n<counter; n++)
        if ((v % arrayp[n]) == 0)
            {
                power1 = log(v)/log(arrayp[n]);
                if (v == pow(arrayp[n], power1))
                    if ((k % (arrayp[n]-1)) != 0)
                        {flag = 0; break;};
            };
    }
else
    {
        for (n=0; n<counter1; n++)
            if ((v % arrayp_mod4[n]) == 0)
                { odd_p = arrayp_mod4[n]; break;};
        if ((odd_p) == 0)
            flag = 0;
        else
            {
                power = (log(v)) / (log(odd_p));
                if (v != pow(odd_p, power))
                    flag = 0;
                else if ((power % 2) != 1) flag = 0;
                else if ((k != (v-1)/2) || (1 != (v-5)/4) || (m != (v-1)/4) ||
                    (b != -1) || (v != d))
                    flag = 0;
            };
    };
return flag;
}

int dual_compl(int v, int k, int d)
{
    int i;
    if (k > ((v-1)/2)) return 2;
    else if (d > v) return 1;
    else return 0;
}

void find_eg(int v, int k, int l, int m, int b, int d)
{
    int i, vprime, power2, result, root, min, r, u, powerm, psi, powern;
    int rprime, tresult, t2result, power3;
    result = 0;
    root = sqrt(v);

```

```

for (i=1; i<counter; i++)                                /*Paley*/
  if ((v % arrayp[i]) == 0)
  {
    power2 = log(v)/log(arrayp[i]);
    if ((v == pow(arrayp[i], power2)) && ((v % 4) == 1)
        && (k == ((v-1)/2)) && (l == ((v-5)/4)) && (m == ((v-1)/4))
        && (b == -1) && (d == v))
      {result = 1; break;}
    if ((root*root) == v)                                /*Example A.1.5(2)*/
    {
      power3 = (log(root))/(log(arrayp[i]));
      if (pow(arrayp[i], power3) == root)
      {
        rprime = k/ (root +1);
        if ((rprime == (root/arrayp[i] -1)) &&
            (l == (-root + rprime*rprime+3*rprime)) &&
            (m == (rprime*rprime + rprime)) &&
            (b == (-root + 2*root/arrayp[i] -2)) && (d == v))
          {result = 7; break;}
      }
    }
  };

if ((root*root) == v)                                    /*PCP*/
{
  min = factorise(root);
  if ((k % (root -1)) == 0)
  { r = k / (root -1);
    if ((r >= 1) && (r <= min) && (l == (root + r*r - 3*r))
        && (m == (r*r - r)) && (b == root -2*r) && (d == v))
      result = 2;
  }
};

if ((v % 4) == 0)                                       /*Example A.1.4*/
{
  u = sqrt(v/4);
  if ((u*u) == v/4)
  {
    if (((u % 2) == 0) || ((u % 3) == 0))
      && ((k == (2*u*u - u)) || (k == (2*u*u -u -1)))
      && ((l == (u*u-u)) || (l == (u*u-u-2))) && (result != 2))
        result = 3;
  }
}

```

```

        if (((u % 2) != 0) && ((u % 3) != 0)      /*Theorem A.2.1*/
            && (result != 2) && ((k == (2*u*u - u))
                || (k == (2*u*u -u -1))) && ((1 == (u*u-u))
                || (1 == (u*u-u-2))))
            result = 5;
    };
};

if ((v % 2) == 0)                                /*Theorem A.2.2*/
{
    powerm = 0; vprime = v;
    do {
        vprime = vprime / 2;
        powerm++;
    } while ((vprime % 2) == 0);
    if (b < -2) psi = 0;
    else if (b < (pow(2, powerm+1) -4)) psi = (b+2)*(b+2)/4;
    else psi = (b- pow(2, powerm) +3)*(pow(2, powerm) -1);
    if (k > (m*(pow(2, powerm) -1) + psi))
        result = 4;
};

if ((v % 8) == 0)                                /*Example A.1.2*/
{
    powern = 0; vprime = v;
    do {
        vprime = vprime / 8;
        powern++;
    } while ((vprime % 8) == 0);
    if ((k == ((pow(2, powern) + 2)*(pow(2, powern) -1))) &&
        (1 == (pow(2, powern) -2)) && (m == (pow(2, powern) +2)) &&
        (d == pow(2, (2*powern+2))) && (b == -4))
        result = 6;
};

/*Example 10.6(1)*/
if ((v==81) && (k==30) && (l==9) && (m==12)) result =8;

switch (result)
{
case 8:
    printf("Example A.1.3\n"); break;
case 7:
    printf("Example A.1.5(2)\n"); break;
};

```

```

case 6:
    printf("Example A.1.2\n"); break;
case 5:
    printf("NOT EXIST by theorem A.2.1\n"); break;
case 4:
    printf("NOT EXIST by theorem A.2.2\n"); break;
case 3:
    printf("Example A.1.4\n"); break;
case 2:
    printf("(%d, %d)PCP\n", root, r); break;
case 1:
    printf("Paley\n"); break;
case 0:
    tresult = t15_1(v, k, l, m, b, d);
    if (tresult == 1)
    {
        t2result = t2_2(v, k, l, m, b, d);
        if (t2result == 1)
            printf("???\n");
        else printf("NOT EXIST by theorem A.2.2\n");
    };
    break;
};
}

int factorise(int root)
{
    int i, *prime, *power, flag=0, min;
    prime = (int*)malloc(sizeof(int));
    power = (int*)malloc(sizeof(int));

/*the for loop is to generate two arrays pointed to by pointers
prime and power, which contain the distinct primes and their powers, to
which the product is the argument root.*/

    for (i=0; i<counter; i++)
        if ((root % arrayp[i]) == 0)
        {
            *(prime+flag) = arrayp[i];
            *(power+flag) = 0;
            do {
root = root / arrayp[i];
            *(power+flag) += 1;
            } while ( (root % arrayp[i]) == 0);

```

```

        flag++;
    };

/*the following is to obtain the minimum of  $\pi^{Ai} + 1$ */

    min = pow((*prime), (*power)) + 1;
    for (i=0; i<flag; i++)
        if ((pow(*(prime+i), *(power+i)) + 1) < min)
            min = pow(*(prime+i), *(power+i)) + 1;

    return min;
}

int t15_1(int v, int k, int l, int m, int b, int d)
{
    /*This function uses an elimination method where the parameters
       are taken to be valid until they passes through the conditions and
       will be returned as not valid if tested correctly*/

    int A, p, u, pi, b1, theta, k11, k12, r, i, vprime, dprime, rootdprime;
    int min, aroot, m11, l11, m12, l12, result=1, resultprime=1;
    int resultprime2=1;
    for (i=1; i<counter; i++)
        if (((v % arrayp[i]) == 0) && ((d % arrayp[i]) == 0))
            {
                p = arrayp[i];
                vprime = v; dprime = d; r=0;
                do {
                    vprime = vprime / p;
                } while ((vprime % p) == 0);
                do {
                    dprime = dprime / p;
                    r++;
                } while ((dprime % p) == 0);
                rootdprime = sqrt(dprime);
                if ((vprime != 1) && ((rootdprime*rootdprime) == dprime))
                    {
                        u = vprime;
                        pi = rootdprime;
                        theta = floor(b/(2*pi) + 0.5);
                        if ((theta + 1)>(b/(2*pi) + 0.5))
                            {
                                b1 = b - 2*theta*pi;
                                A = (u+b1)*(u+b1) - (pi*pi - b1*b1)*(u-1);
                            }
                    }
            }
}

```

```

aroot = sqrt(A);
if (aroot*aroot == A)
{
    if (k<u) min = k; else min = u;
    k11 = (u + b1 -aroot)/2; k12 = (u + b1 + aroot)/2;
    m11 = k11 - ((pi*pi - b1*b1)/4);
    m12 = k12 - ((pi*pi - b1*b1)/4);
    l11 = b1 + m11; l12 = b1 + m12;
    if ((k11> min) || (k11 < 0)) resultprime = 0;
    if ((k11 != 0) && (k11 != u-1))
        if ((l11 < 0) || (m11 < 0) ||
            ((u - 2*k11 + l11) < 0) ||
            ((u - 2*k11 -2 + m11) < 0))
            resultprime = 0;
    if ((p >= 5) && ((k11 != 0) && (k11 != u-1)))
        if (((r % 2) == 1) || ((theta % (p-1)) != 0)) &&
            ((r % 2) == 0) || ((theta % (p-1)) != (p-1)/2)))
            resultprime = 0;
    if ((k12> min) || (k12 < 0)) resultprime2 = 0;
    if ((k12 != 0) && (k12 != u-1))
        if ((l12 < 0) || (m12 < 0) ||
            ((u - 2*k12 + l12) < 0) || ((u - 2*k12 -2 + m12) < 0))
            resultprime2 = 0;
    if ((p >= 5) && ((k12 != 0) && (k12 != u-1)))
        if (((r % 2) == 1) || ((theta % (p-1)) != 0)) &&
            ((r % 2) == 0) || ((theta % (p-1)) != (p-1)/2)))
            resultprime2 = 0;
    if ((resultprime2 == 0) && (resultprime == 0))
        result = 0;
    } else {result = 0; break;};
    } else break;
    } else break;
};
if (result == 0)
    printf("NOT EXIST by Theorem 4.1.1 with p = %d\n", p);
return result;
}

int t2_2(int v, int k, int l, int m, int b, int d)
{
    int pro1, pro2, t, s, star, psi2, i, result;
    result = 1;
    for (i=0; i<counter; i++)
        if (((v % arrayp[i]) == 0) && (d % arrayp[i] == 0))

```

```

{
  pro1 = v; pro2 = d; t=0; s=0;
  do{
    pro1 = pro1 / arrayp[i];
    t++;
  } while ((pro1 % arrayp[i]) == 0);
  do{
    pro2 = pro2 / arrayp[i];
    s++;
  } while ((pro2 % arrayp[i]) == 0);
  if ((pro1 != 1) && (pro2 != 1) && ((s % 2) == 0))
  {
    if (arrayp[i] == 2) star = s/2 - 1;
    else if ((arrayp[i] % 2) == 1) star = s/2;
    if ((pow(arrayp[i], star) - 1) == 0) continue;
    else {
      if (b < (-1*pow(arrayp[i], star))) psi2 = 0;
      else if (b < (2*pow(arrayp[i], t) - pow(arrayp[i], star) - 2))
        psi2 = (b + pow(arrayp[i], star))*(b + pow(arrayp[i],
          star))/4;
      else
        psi2 = (b - v/pro1 + pow(arrayp[i], star) + 1)*(v/pro1 - 1);
      if (k > ((m*(v/pro1 - 1) + psi2)/(pow(arrayp[i], star) - 1)))
        {result = 0; break;}
    }
  }
  } else break;
};
return result;
}

```

Bibliography

- [1] I.M. Chakravarti. 1969. Partial difference sets, calibration designs and error correcting codes. *Bull. Inter. Stat. Inst.*, 43(2): 104-106.
- [2] R.C. Bose and J.M. Cameron. 1965. The bridge tournament problem and calibration designs for comparing pairs of objects. *Journal of Research of the NBS-B, Maths. and Math.Phys.*, 69: 323-332.
- [3] S.L. Ma. 1994. A Survey of Partial Difference Sets. *Designs, Codes and Cryptography*, 4: 221-261.
- [4] K.M. Ng. 1994. Partial Difference Sets. *Honours Thesis*
- [5] S.L. Ma. 1984. Partial Difference Sets. *Discrete Mathematics*, 52: 75-89.
- [6] S.L. Ma. 1997. Some necessary conditions on the parameters of partial difference sets. *Journal of Statistical Planning and Inference*, 62: 47-56.
- [7] K.Ireland and M.Rosen. 1982. A Classical Introduction to Modern Number Theory, Springer.
- [8] R.A. Bailey and D. Jungnickel. 1990. Translation nets and fixed-point-free group automorphism. *Journal of Combinatorial Theory Series A*, 55:1-13.
- [9] T.Beth, D.Jungnickel, H.Lenz. 1999. Design Theory, Vol 1, 2nd ed. Cambridge University Press